Secure Collaboration in Onboarding

Pratap Chillakanti

School of Science and Technology

Middlesex University

A thesis submitted in partial fulfillment for the degree of

Doctor of Philosophy

August 2013

Dedication

To my two sets of twins who make my life meaningful every single day

Mukund (Muku Beta) and Kartik (ET)

Mahima (Mahi) and Kirthi (Kheer Baby)

And

To their lovely and extraordinary mother who continues to raise our children in exemplary fashion

Chaya

Guru Vandanam

(Respectful Obeisance to my teachers)

Guru Brahma Guru Vishnu
Guru Devo Maheswaraha
Guru Saakshaat Para-Brahma
Tasmai Shri Guruve Namaha

As I complete this milestone and move on to the next, it just feels right and immensely satisfying to offer my obeisance to all my teachers who enabled this journey. I offer obeisance to my very first teacher, (late) Professor CVS Rao, my father. Father, you are the inspiration for my pursuit of academic education in Electronics and Communication Engineering and later Computer Science. You have given me countless pearls of wisdom but a few things that I remember most are the sense of duty toward family and toward students, and the importance of keeping good company with wise people so I can hope to grow from a stupid young man to a wise old man eventually. Well, I think I am on the right track. As I promised to you just before your wonderful soul moved on, I am finally submitting my PhD thesis. As you said so often, do the best that you can and leave the result to God. Well, here I am following your sage advice. I offer obeisance to my mother who has raised me and from whom I have learned how to be compassionate and kind in taking care of family members who are in distress and require a helping hand.

I offer obeisance to my teachers in school at St. Paul's and Railway Junior College who have laid the foundation for my academic pursuits. My fading memory recalls Ms. Franey, my English teacher from primary school, Mr. Rasool sir and Mr. Gopala Krishna Murthy from Railway Junior College, my two very best Math teachers who sparked my career interest in Engineering, Ma Reddy sir, who taught me my mother tongue Telugu, and of course my principal at St. Pauls', Brother Stanislaus, who has been an inspiration for all students to dream! I fondly remember the one and only instance of scolding that I received from him (in those days scolding included a cane!) for not performing to my potential. Brother Stanislaus, this is a great life lesson learned from you. Whenever I procrastinate, your words come to my mind. This milestone is in your honor brother!

I offer obeisance to my teachers in Engineering at my undergraduate University, JNTU, and Computer Science and Engineering teachers at my post-graduate institution, Osmania University. I have gained lifelong knowledge and wisdom from Professors GR Babu, Paradesi Rao, Lal Kishore, Narasimha Murthy, Gopal Reddy and so many more. These teachers have taught me much more than the academic subjects. I fall back upon the nuggets of wisdom that I gained from them as I perform my duty toward my students and to society.

I offer obeisance to my teachers at Middlesex University. Professor Tully, thank you for accepting me as your student. The completion of this thesis is in your honor too. The last conversation we had was one of optimism and a sense of purpose to move toward the goal of completing my thesis. Your words carried me through the challenging times that I have faced in the last few years. I am sure I have your blessing

from up above as I complete this milestone. I offer my thanks to Dr. Geetha who kindly took over as supervisor and prodded me to complete this in honor of my father and Professor Tully. Geetha, I am so privileged and lucky to have worked with you. I offer my thanks to Ms. Elli who has so kindly shared her knowledge and wisdom about how to put together a thesis based on many finer nuances of conducting research. Elli, I consider you my angel who made this happen!

I offer obeisance to my mentors, colleagues, and friends as well. Joe, you have taught me what it means to be a consultant besides also teaching me how to think through situations. Steve and Stan, you have showed me how to be a good teacher! I am truly blessed to have you come into my professional life and guide me. Tony, you paved the way for my success that allowed me to dream about Lensoo and realize the vision of bringing technology innovation in learning and teaching. Vish, I am blessed to have your guidance and support as I try to create a success story for Lensoo. I continue to gain valuable knowledge and wisdom from you. My good friends from college, Vidya, Narayana, Murali, Uma have inspired me is many ways. Vidya, I recall your statement from our college days in late 1970s: “I know I am smart.” I realized later that it is essentially self-belief. Murali, time spent with you, whether visiting the Hanuman temple or learning from you, has always been enjoyable. Your music is something that I always cherish. Narayana, thanks for teaching me when we were preparing for our exams. I fondly remember the dal rice that you used to cook. Uma, you have been my very good friend and one of the nicest people who I have ever met. Time spent with you just hanging out is a cherished memory and I am glad we are collaborating at the moment to make a difference in education. Uday, my good friend who came into my life has been a true friend in more ways than one. Uday, I learned sincerity from you be it work or be it in anything else. I am so glad that we both share the same passion for the three T’s: Truth, Technology, and Training.

I offer obeisance to my most beloved professor, C.V. Ramamoorthy. He is one of my two role models, the other being my father. Professor Ram, I have learned what humility is all about from you. You accomplishments are many; yet your kindness toward your students and your gentle guidance is something that every teacher could learn from. You have produced 75 PhD graduates and you have constantly reminded me about reaching my milestone. Without your inspiration and guidance I would not have come this far in submitting my thesis. I hope that soon you can say that I am your 76th PhD graduate.

I offer obeisance to the biggest teacher of all, Life. I have made many mistakes in life be it in terms of hurtful words, actions, and reactions. Life has taught me how to be kind, how not to use harsh words and it has taught me how to be a compassionate human being. Life has also taught me that pursuit of happiness is really pursuit of passion.

Acknowledgements

This research undertaking was made possible because of my colleagues at Cisco who have given me an opportunity to work on projects that allowed me to gain insights into security issues in general and access control management issues in particular. I am deeply grateful to Tony Rogers who sponsored my research undertaking by including me in several initiatives. I also thank the wonderful industry colleagues and friends Bridget, Christine, Farrukh, Tim, Sean, Rik, and others who have provided me an enriching work experience that led to insights in collaboration security.

I thank the many people who have so kindly agreed to participate in a survey when I needed to collect data in the context of this research. Without their timely assistance, it would not have been possible to accomplish this milestone. I thank Mike Rogers and Fred Becker, who have spent time with me for a formal interview. This has given me deep insights into onboarding processes and issues in access control management in onboarding.

I thank my supervisors, Prof. Ramamoorthy, (late) Professor Tully, Dr. Geetha, and Ms. Elli who have guided me in this research. Their insights and their constant encouragement were critical in reaching this milestone. I sincerely thank Elli and Geetha for finding time to review and provide feedback. I thank Professor Chris who gave me time and calibrated my insights into self-organizing systems. I take this opportunity to thank Professor J.K. (Jake) Aggarwal at University of Texas at Austin who was my Professor and Mentor when I embarked on this journey. He is someone who continues to inspire me. I thank my manager at HP, Brian Sakai, who gave me the opportunity to go to University of Texas at Austin.

I thank my four wonderful children who are curious about when I would finish. I hope that this milestone would encourage them to pursue higher levels of academic excellence. Finally, I thank my spouse who has gone through many challenges in life with me but always ensured that kids grew up well. She is simply the best mother on earth as far as I am concerned. God bless her.

Abstract

The process of onboarding a company is characterized by inter-enterprise collaboration between the acquiring and the acquired companies. Multiple cross-functional teams are formed to assimilate and integrate the processes, products, data, customers, and partners of the company under acquisition. Dynamic access control management in such inter-enterprise collaboration is the subject of this thesis.

A problem in inter-enterprise collaboration in onboarding is that information assets shared by collaborating teams are not adequately protected. As a result, there is potential for accidental or malicious leakage of sensitive business information like the intellectual property, product roadmaps and strategy, customer lists etc. Also, the statically defined access control policies are not sufficient to address access control requirements of dynamic collaboration where there is a constant change in people, processes, and information assets in collaboration repository. This research proposes a new approach and model to integrate security in onboarding collaboration process.

Research methods such as, literature review, field studies including direct experiential projects in onboarding and interviews with experts in Mergers and Acquisitions, and detailed data collection and analysis through surveys are used to identify the issues that need to be addressed in the onboarding process. Literature review enabled the identification of access control requirements from the perspective of statically defined policies and the need to determine access dynamically. From the field studies, it was deciphered that there is a need for a well-defined onboarding collaboration process. The data analysis and interpretation from the survey results provided insights into the needs for integrating security in all phases of onboarding collaboration. All these research methods essentially enabled identification of two key issues that this research addresses: 1) well-defined onboarding collaboration process and 2) building security in all phases of onboarding collaboration.

A new approach and model called SCODA is developed to integrate security in all phases of onboarding collaboration. Onboarding collaboration process consists of four phases: create, operate, dissolve, and archive. These phases provide the basis for

systematically addressing security and access control when the collaboration team is formed, while it is operating, when the team is dissolved after completing its tasks, and when shared information assets are archived. The research adapts role based access control (RBAC) and formally defines the enterprise, functional, and collaboration roles for making access control management decisions. New ideas are developed in trust-based access control management in dynamic collaboration. The change management aspects are also discussed. The SCODA model is validated and the refinements incorporated accordingly.

This research contributed to both theory and practice of information security in general and access control in particular in the context of dynamic collaboration. It proposed a new approach of building security in, i.e. to integrate security in all phases of collaboration. In order to build security in, a new onboarding collaboration process is developed that is adaptable and customizable. It has also developed a new approach for trust based dynamic access control based on the new concepts of strong and weak trust relationships. These trust relationships are also adaptable and customizable.

Finally, this research has potential for future research work in the design and implementation of multi-paradigm based enterprise security frameworks and inter-enterprise collaboration.

Table of Contents

Figures and Tables

1 Introduction

"Intellectuals solve problems; geniuses prevent them." – Albert Einstein

1.1 Introduction

Access control management in inter-enterprise collaboration, in the context of mergers and acquisitions (M&A), is the primary focus of this research. In today's interconnected global economy, mergers and acquisitions have been growing rapidly [1]. There are many common motivations for mergers and acquisitions such as to increase customer base, expand the product offerings, expand global presence etc. [2]. This research addresses the scenario where a company acquires another company. From the time the letter of intent to purchase is accepted to the time the assimilation and induction of people, processes, technologies, tools, customers, partners, suppliers and others is completed, both the companies involved go through a series of tasks to manage the acquisition smoothly. Many functional organizations such as the engineering, finance, marketing, sales, channels, customer support, training, and IT are involved in this complex undertaking. In order to manage this complexity, a cross-functional team is usually put in place dynamically to manage all aspects of this assimilation which is termed as *onboarding* in industry accepted terminology. Onboarding is also commonly used in the industry to discuss employee onboarding from a human resource and development perspective.

In essence, there is collaboration between the two companies. From a business perspective, collaboration is the act of working together to achieve a business objective. The business dictionary defines it as, a cooperative arrangement in which two or more

parties (which may or may not have any previous relationship) work jointly towards a common goal [3]. In the case of onboarding, a cross-functional team from both the acquiring and the acquired company work together to achieve the business objective of assimilating the people, processes, technologies etc. of the two companies. When a team is put together, there are numerous tasks that would take place such as selecting the team members, assigning roles and responsibilities, creating the necessary infrastructure to coordinate, communicate and cooperate. A significant component of this team dynamics and collaboration is sharing a variety of work artifacts and documents spanning engineering, financial, legal, sales and marketing, and IT. In addition, these teams share processes, methods, tools, and applications. All of these are broadly termed as information assets.

Information security is a key aspect of such dynamic inter-enterprise collaboration where business sensitive information is shared among a group of people as well as processes. Information security deals with various trust aspects of information. It is not specific either to computer systems or to information in electronic form; it applies to all aspects of safeguarding or protecting any form of information or data. The US National Information Systems Security Glossary [4] defines information systems security (INFOSEC) as:

> *the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.*

There are many different nuances of information security. As discussed in [5], it has been viewed as synonymous with computer security, computer and network security, information technology (IT) security, information systems security, or information and communications technology (ICT) security. Though each of these has a different emphasis, the common issue that they address is the security of information. It is generally accepted that they are all subsets of information security [6]. In other words, information security addresses not just information but all infrastructures that facilitate its use — processes, systems, services, technology etc., including computers, voice and data networks etc.

In the context of mergers and acquisitions and the resulting inter-enterprise collaboration, information security from the perspective of managing access to shared artifacts must be addressed because information must be protected against unauthorized access, thus preventing either accidental or malicious misuse of information. It is this aspect of secure collaboration, access control that is the focus of this research.

As mentioned earlier in this chapter, onboarding entails assimilation of people, process, and technologies. In this process of assimilation there is potential for change in all these three dimensions. For example, roles and responsibilities for people may change, new roles could be defined, and multiple roles could be merged. The same applies to processes as well as technologies. Of particular interest to our research is the change management aspect associated with secure collaboration. For example, how would access control be managed in terms of setting up and modifying roles, privileges, and

trust? The practical nature of administering a variety of systems, frameworks, processes etc. requires that one should design and develop these in such a way that they are easy to use and administer in terms of changes [7]. Addressing change management is an integral component of this research.

1.2 Purpose

The purpose of this research is to investigate the subject of access control management in onboarding in the context of mergers and acquisitions (M&A). Though access management in the context of collaboration has been researched in general in [8], [9], [10] etc., (note: detailed references cited and discussed in the chapter on literature survey and analysis), this investigation has not found evidence that it has been addressed systematically in onboarding in the context of M&A. The nature of collaboration in this context is that the people who come together to manage onboarding come from different functional units, different organizations, and they have different processes, methods, and tools that they use. The M&A type of inter-enterprise collaboration requires further research compared to traditional inter-enterprise collaborations that have been studied because the context of M&A brings with it its own nuances such as 1) the transient nature of collaboration – once the merger/acquisition is complete, the inter-enterprise team is dissolved, 2) the merger may or may not be friendly in which case there is more scope for abuse/misuse of sensitive information, and 3) security management is more dynamic - authorization to business sensitive information assets may have to be granted in ad-hoc manner (meaning there may not be pre-defined authorization rule to determine access). This research also addresses change management in the context of secure collaboration.

1.3 Overview of Research

This research will bring four specific aspects together to provide a foundation for access control management in onboarding. First, industry experience in participating in onboarding activities and literature survey of mergers and acquisitions will provide insights into the complex nature of onboarding. Though the process of assimilating the acquired company seems to be functional, preliminary investigation shows that access control management aspects in the context of dynamic collaboration have not been addressed explicitly as integral to the acquisition process. Second, literature review of information security field has shown that access control management has been addressed in the context of dynamic collaboration. However, this investigation did not discover any significant research in access control management in inter-enterprise secure collaboration in the context of M&As. In this type of inter-enterprise collaboration it is not very clear as to what type of access control management models must be used to manage secure collaboration. Third, literature survey of self-organizing systems suggests that one can view the inter-enterprise collaboration team in onboarding as self-organizing. This observation leads us to further researching access control management in onboarding based on the concepts of self-organization. Fourth, the literature review of collaboration trust models provides insights into the notion of trust in addressing security in inter-enterprise collaboration. This research investigates the adaptability of the notion on trust in access control management in the context of onboarding.

1.4 Research Objectives

Literature review and analysis show research gaps in the literature on onboarding, in the context of M&As. More specifically, the gaps are in access control management in inter-enterprise collaboration in the context of onboarding. This research further discovered the potential of adapting the concepts of self-organization, and trust models developing access control management in onboarding. Based on these preliminary results, the research objectives and deliverables are the following:

- Development of an access control management model for secure collaboration in onboarding.
- Address change management that accompanies access control management model in on boarding.

1.5 Thesis Outline

Chapter 2 presents an overview of onboarding in the context of mergers and acquisitions. The term *onboarding* is used in the commercial and corporate world to usually mean a process to assimilate and integrate new employees into an organization [11]. The focus of this chapter is to define onboarding in the context of this research and to discuss the process of onboarding an acquired company. The focus of chapter 3 is literature review and analysis of access control management, self-organizing systems, and collaboration models. This chapter will include an analysis of how research contributions from these fields will be used in the development of access control management model for inter-enterprise collaboration in onboarding. The focus of chapter 4 is research methodology and research design used to produce and validate

the results. Chapter 5 discusses the data collection and analysis of survey results. Included in this chapter are the preliminary survey and the final survey, data analysis and interpretation of results which influence the development of access control management model. Chapter 6 discusses a new access control management approach for secure onboarding collaboration. It adapts role based access control (RBAC) model, and proposes new concepts of enterprise, functional, and collaboration roles. A new secure onboarding collaboration process model, SCODA (a process of integrating Security in Create, Operate, Dissolve, and Archive phases) is developed for addressing security across the onboarding collaboration lifecycle. This chapter also discusses perspective of self-organization in access control management in dynamic collaboration. In addition, it discusses how trust management plays a role in access control management in in onboarding collaboration. Finally, in the same chapter, the change management aspects of access control management in onboarding are discussed. Chapter 7 focuses on model validation with experts and the updated access control model. Chapter 8 discusses the research contributions and significance. It will include a discussion on future research directions in access control and security management in dynamic collaboration.

2 Onboarding

"When you know better you do better." -- Maya Angelou

2.1 Introduction

Onboarding is a relatively new term. It has been used in the literature most often to discuss the orientation and socialization of a new employee hire in a company [12]. In this context, as discussed in [13], onboarding is viewed as a process of learning, networking, resource allocation, goal setting and strategizing. The end goal of this process is to have the new employee reach maximum productivity quickly [14]. In the context of mergers and acquisitions, one of the perspectives proposed in the literature is to view the assimilation of the acquired and acquiring companies as a process of *task integration* and *human integration* [15]. Traditionally, the research in organizational behavior focuses on behavioral implications of acquisitions at both the individual and organizational levels. It emphasizes the importance of generating satisfaction and eventually a shared identity among the employees of both organizations. This is called the *human integration*. The process perspective is focused on the actions taken by management to guide the post- acquisition integration process. It views *task integration* as the objective of the acquisition, measured in terms of transfers of capabilities and resource sharing. The success of acquisition is dependent on both task integration as well as human integration.

The employee onboarding is further discussed in the literature by various researchers. For example, in [16], the case is made that it is important for a company to make a positive impact on new hires because these employees make their decision to either

leave or stay with a company in the first six months. The financial impact of lack of formal onboarding processes is discussed in [17]. The questions that enable maximizing employee onboarding efforts are presented in [18]. In essence most of this literature on employee onboarding suggests that formal on-boarding processes positively impact new employees in numerous ways: the unknowns are answered, expectations and goals are set, they are more easily assimilated into the organization's culture and they build strong relationships faster [13]. The key characteristics for successful employee onboarding were identified, as shown in Table 2.1.

Table 2-1: Characteristics of successful employee onboarding

Characteristics	Comments
Clearly defined organizational objectives [11]	vision, mission, product and solutions, culture, organization chart, go-to people (people who can help) etc. are presented
Onboarding process begins as soon as the person accepts the offer [14]	creates the impression that the company is caring and supportive
Define Metrics that Matter (MTM) [11],	turnover rate, productivity, employee satisfaction etc. Facilitates continuous process improvement
Leadership buy in and support [14]	executive management support in allocating time, money, and resources
Employee expectations and goals defined collaboratively [19]	employees know their role and responsibilities
Mentors assigned [19]	the go to people for an employee to enhance his/her career development
Manager's performance objectives include onboarding [12]	employee's immediate manager knows his/her responsibilities in ensuring success of a new hire
Technology Innovation [19]	adapting technology innovation for providing a holistic onboarding experience
New hire social community [12]	providing a community support portal throughout onboarding
Formal training processes [14]	blended training and community support to enable employee learn about the company's people, products, solutions, customers, competition etc.
Implement formal surveys throughout onboarding [19]	employee satisfaction surveys done throughout the onboarding cycle

Though employee onboarding is a well-researched topic in the literature, not much research addresses acquisition onboarding and its access control management challenges. Employee onboarding is one of many important aspects of acquisitions. The literature identified is primarily concerned with Mergers and Acquisitions from a management perspective whereas very little is present from a technology perspective, especially from the viewpoint of collaboration security. In order to address these security issues, it is important to first understand the process lifecycle of onboarding companies. This provides a reference framework to study collaboration security because it will facilitate the identification of objectives, roles, responsibilities, information shared among the collaborators, relationships, security risks, and change management issues. The next section is devoted to a discussion on understanding acquisitions and process lifecycle for onboarding companies.

2.2 Process Lifecycle for On Boarding Companies

Acquisitions are considered as a way for implementing a business strategy focused on growth [2]. The acquisition lifecycle begins with the business plan and culminates in the acquisition and onboarding of the company that is acquired. Researchers have identified numerous phases of acquisition lifecycle. In [2], the author proposes a 10 phase acquisition process:

1. Business Plan
   Develop a strategic plan for the entire business
2. Acquisition Plan
   Develop an acquisition plan that is aligned with business strategy
3. Search Pre-purchase decision activities
   Search for potential companies for acquisition
4. Screen

Short list the potential companies

5. First Contact

   Initiate contact with the target company

6. Negotiation

   Agree on valuation of the target; perform due diligence, develop financing plan

7. Integration Plan

   Develop plan for integrating the acquired business

8. Closing

   Obtain necessary approvals and execute closing from a legal perspective

9. Integration

   Implement post-closing integration

10. Evaluation

    Conduct Post Closing the success of acquisition

Another perspective on acquisition lifecycle is discussed in [20]. The steps of acquisition process discussed are very similar to the above. Based on the literature review and analysis of various acquisition lifecycles, it is inferred that collaboration security is potentially addressed at three process steps in any process lifecycle for acquisitions 1) forming an acquisition team, 2) integration planning and 3) forming an integration team. These steps come after a company has given a formal letter of intent to acquire another company and both the companies have agreed on the acquisition. An acquisition team is formed to move the process forward. Collaboration security must be addressed when the acquisition team is formed as the team members will be accessing a variety of business sensitive information. The acquisition team will continue to exist until the integration is complete. Another milestone that is triggered after both companies agreed on the acquisition is the formation of integration planning team. This step also entails addressing collaboration security because there will be an inter-enterprise team collaborating and sharing business sensitive information. The formation of integration

team is another significant milestone where members from both companies form a collaborative team to plan and execute integration strategy. Typically, integration team size is larger than the size of the acquisition team as well as the integration planning teams. This is because in this step, resources from IT, and first level business and project members will be involved in looking at merging the IT and the business processes [21]. This is perhaps the most critical phase where security must be addressed as members have access to numerous business sensitive documents and other artifacts that if compromised may pose high business risk.

2.3 Onboarding Insights

Though companies like Cisco, GE, and Intel have a fairly well defined process for managing acquisitions, the access control management in inter-enterprise collaboration is something that could be improved and enhanced. First-hand experience in onboarding and interviews with experts suggest that the members of acquisition, integration planning and integration teams have access to many documents though their role does not entail such access privileges. Furthermore, beyond the usual post-mortem analysis that comes after the onboarding is complete, there are no well-defined feedback loops which are integrated into the process of onboarding, especially in the context of security management. In addition, due to lack of collaboration security controls at integration phase it is not known if any security breaches occurred which were either intentional or unintentional. Research shows that more than 60% acquisitions fail to deliver value and often, it is employees who are not happy with the acquisition. Lack of security controls in managing access to information repository poses significant business risks such as financial loss, IP theft, sales data theft, and

other business critical data loss. Chapter 5 (Data Collection and Analysis) presents more insights in access control management in inter-enterprise collaboration in onboarding.

2.4 Research Context and Focus

The context of this research is onboarding acquired companies. The rate of acquisitions in the new millennium is steadily increasing while at the same time the global competition is increasingly becoming more challenging. These developments create an environment in the workplace that demands increase security measures in all aspects of running a business. The increasing cyber-attacks are one example of such security threat. Security is about managing risks. This implies that at all points of time in the existence of a business there must be sufficient access control mechanisms in place to safeguard a company's assets.

Acquisitions have been studied in academia and industry predominantly by researchers in management, finance, economics, sociology, and accounting domains. They have employed a rich and diverse set of methodologies to examine acquisition phenomena. Although this work has uncovered numerous notable findings, few attempts to synthesize these insights across fields have emerged [22]. In these domains active research is going on in the areas such as *Antecedents to Acquisitions*, *Consequences of Acquisitions*, *and Human Capital Management*.

This research adds a new dimension of security to the field of acquisitions. In the overall acquisitions process, the focus is on access control management in dynamic collaboration in onboarding. An integrated focus is to address change management in

the context of access control management. In the next chapter, a detailed literature review is presented with emphasis on evolution of access control models, self-organizing systems, and access control management in dynamic collaboration.

3 Literature Review

"Know what you are talking about." -- John Paul II

3.1 Introduction

Access control management in inter-enterprise collaboration, in the context of onboarding, is the primary focus of this research. The process of onboarding acquired companies entails people from both the acquiring company and the acquired company working together to ensure that people, processes, technologies, partners and customers are systematically integrated. This scenario of people working together requires cooperation, coordination, and communication among the team members. In the industry, this is usually referred to as collaboration between the two companies for successful integration. One facet of such collaboration is the need for people to share many types of documents and other working artifacts like customer and partner lists, financial reports, engineering diagrams, product roadmaps etc. This type of information is highly business sensitive and poses a security risk to companies as measured in loss of revenue, competitive advantage, reputation, legal, and otherwise . In the realm of the onboarding context, one has to also address access control issues pertaining to information access. For example, not everyone on the onboarding team requires access to customer lists. Perhaps, this is required only for those members whose functional role pertains to sales and marketing. Another facet of onboarding is the dynamic nature of the team composition. During the lifecycle of onboarding, different cross-functional team members play an active role in the acquisition process and once the tasks pertaining to that part of the lifecycle are complete, their role ends. Essentially, the team structure is dynamic during onboarding collaboration. Access control management in such a

dynamic collaboration environment becomes an important element of successful onboarding. This research also aims to adapt concepts from “self-organizing systems” to study access management in dynamic collaboration. References to the concept of self- organization became common place in the scientific literature beginning in the 1970’s when scientists researched complex systems [23]. Change management is another important facet of integrating the people, processes, and technologies in the context of onboarding. For example, new roles may be discovered, existing roles may be combined, processes could be modified etc. This research aims to address change management in the context of onboarding. This chapter first presents an evolution of security and access management. Next, the evolution of collaboration security is presented. This chapter also includes a discussion on self-organized systems as it is applicable to this research.

3.2 Evolution of Security and Access Control Management

Access control deals with controlling access to information. According to Sandhu [24] well known for his pioneering research in information security research and Role Based Access Control model, the purpose of access control is to limit the actions and operations that a legitimate user can perform in a computer system. Ever since the development of the first scientific computers in late 1950’s, there has been an interest in access control management. The field was known as computer security and it dealt with the management of access to computers and the information stored in them. Computer security as a discipline began in earnest in the 1970’s [25]. It has evolved with advances in computing beginning with mainframes in the 1950’s to the current environment driven by distributed computing, internet, collaboration, and social network

technologies. The subject area of security has branched off into different research directions in the process. Table 3.1 depicts this evolution.

Table 3-1: Evolution of Security Research

Time	Technology	Applications	Security Research Focus
1950s	Mainframe	Scientific	Physical access, Computer Cryptography
1960s	Minicomputers	Business Data Processing	Operating Systems Security, Access Control Matrices, Information Security
1970s	PCs, LANs	Database Processing, Rudimentary PC based applications	CIA model of information security, information flow analysis based security
1980s	Client-Server, LAN/WAN	Desktop Applications, Client-Server Applications	Network Security, Database Security
1990s	Distributed Computing, Internet	Enterprise Resource Planning Applications, First Generation E-commerce Applications	Application Security, Information Security
2000+	Mobile Computing, Holistic Ecosystem	Mobile Applications, IP Telephony, Collaboration systems, Web 2.0	Enterprise Information Security, Mobile Security, Software Security, Risk analysis based security approaches, Collaboration security
2010+	Social Networking, Mobile Apps	Community sharing, Smart Phones and Apps	Social networking security, App security

The evolution of computer security can be mapped to the evolution of computing technology, beginning with mainframes, progressing to a few networked minicomputers

in one office, further evolving into a geographically distributed client – server environments, and today spanning global networks of computers connecting businesses, partners, vendors, customers, and more. Along with the advances in computing environments, the security issues addressed by the research community evolved too. A new dimension was added to this picture. As the power of computing evolved, the size and complexity of applications harnessing the computing power evolved too. Starting with simple scientific applications, we have progressed to data processing applications on mainframes in the 1960's to using desk to applications in the 1980's. Today, we are using web enabled enterprise applications that are universally accessed by a variety of entities and people including businesses, customers, partners, vendors, and others. The evolution of applications has added an entirely new dimension to security. In fact, the very nature of computer security has changed dramatically. It has resulted in different branches of study including operating systems security, network security, database security, application security, mobile security, and software security. Figure 3.1 shows the evolution of the branches of security.

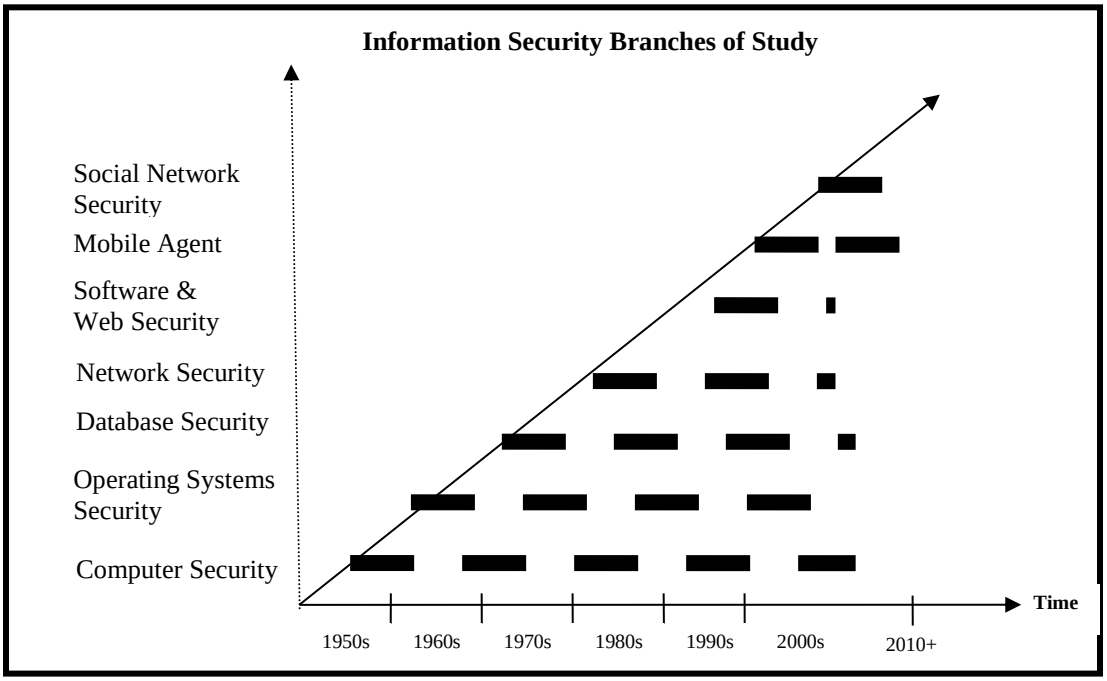


Figure 3-1: Evolution of Security Branches of Study

The purpose of Figure 3.1 is to depict the evolution of the information security field. It can be argued that there are other branches of security as well; for example, programming language security. However, for the purpose of this research, these branches are shown, as they are relevant to put the research in context in the sense that access control management is studied at different levels of abstraction. In addition, this depiction closely models the computing paradigm where we have Hardware (computers), Operating Systems, Networks, Databases, Software & Web Applications, Mobile Applications, and Social Networking. We can clearly see the progress of the security branches of study. First came computer security in the 1950's, where the prominent research focus was on cryptography [26] followed by operating systems security in late 1960's [27]. The 1970's witnessed maturing database processing paradigms and the associated database security frameworks in mainframes and minicomputers [28]. The advent of PCs in late 1970's, and the birth of Local Area

Networks expanded the scope of security and resulted in network security branch of study [29]. The 1980's witnessed true client-server distributed applications spread over LANs/WANs and the network security field of study expanded rapidly [30] . It was also the time that access control issues took on a new dimension as computing was spread over a distributed network; security came into more focus in the industry, and the Chief Information Officers in the industry began to talk about an information security strategy encompassing all aspects of computing.

The rest of the section presents the evolution of security and access control models categorized into 1) Early Phase: Access control and information flow models, 2) Second Phase: Access Control Lists, Role based and Trust based Models, 3) Next Generation: Innovative Security Strategies, and 4) Most Recent Phase: Social Networking and Cloud Computing Security

3.2.1 Early Phase: Access Control and Information Flow Models

Most of the initial research contributions in access control came from the operating systems subject area. The pioneering research of Lampson [31] resulted in perhaps the most intuitive as well as significant access control model using *access control matrix*. This model was later refined by Graham and Denning [32]. Access Control Models control access to information. They were first proposed in describing the protection features in Operating Systems. The key conceptual elements of the access control matrix are the Subject, Object, and the Rights that the Subjects have over the Objects (protection state). In addition, these models have a set of rules for changing the protection state of the system. Each column in the matrix corresponds to an object, and each row corresponds to a Subject. A Subject is an activity entity that corresponds to a

user or process, an Object is something that we want to protect. The cell that corresponds to the intersection of the Subject and Object depicts the rights that a Subject has over the Object. Figure 3.2 illustrates an access control matrix.

Table 3-2: Illustration of access control matrix

User/Resource	File 1	File 2	File 3
Tom	Owner, R, W	Owner, R, W	R
Dick	R	R, W	R
Harry	R, W	R	Owner, R, W

User Tom is the Owner of File 1 and File 2 and he has both Read (R) and Write (W) access to his files. The rest of the table is self-explanatory. The HRU model by Harrison et. al. [33] demonstrated significant fundamental results in the expressive power of models based on access control matrices. Bell-LaPadula model [34] is another seminal early research work in the area of access control. This model is primarily based on military style classification. In this classification scheme all objects are categorized into compartments based on their perceived importance and sensitivity. The confidentiality policies are enforced by controlling the information flow. In essence, this model has a set of rules that prevent the flow of information from a sensitive object to another object at a lower sensitivity level. The Biba Integrity model [35] refines and adapts the Bell-LaPadula model for commercial purposes. It is important to note that during the early days of computer security, it was a primary concern for government and military organizations and the proposed research models reflected the security requirements of these organizations.

In addition to these models, a number of other access control models were proposed. Some of the models well known in the literature are the take-grant model [36], SPM Model [37], CPD model [38], Types Access Matrix Model [39], and ESPM model [40]. Some of these models, for example the take-grant model, answer the safety question: *is a particular state reachable from the initial state?*

Though the access control models are effective in reasoning about protection features of operating systems, they are not particularly effective in reasoning about *information flow*. As defined by Denning [41], information is said to flow from object A to object B if the value of object B depends on the value of object A. The security models based on information have been formalized using the notion of state machines that lead to the concept of *information flow predicates* defined in terms of *traces* in a system. A trace is a possible sequence of inputs and outputs pertaining to the operations of a system.

The basic foundation of information flow analysis is the operations and their effect on data. Information flows from one data object to another data object if a change in the first object causes a change in the other object. The operation that causes this change is said to cause the information flow. Information flows can be explicit (assignment statement) or implicit (conditional statements) [42]. Further, the information flows can be because of functional dependencies ($X \rightarrow Y$), meaning the value of Y is dependent on the value of X, or deductive reasoning (knowing the value of X implies knowing the value of Y). In essence, if an information flow exists between object A and object B, an input to object A causes changes in output of object B. This concept is captured as follows [42]:

Axiom 1: Basic Information Flow Axiom

A flow, X ⟶ Y occurs only when the value of Y is updated

Definition: Flow

A flow, denoted X ⟶ Y, takes place from an object X to another object Y if object Y contains information about object X after execution of some program that involves both objects.

The components of an information flow model are [41]:

- A lattice
- A set of labeled objects
- The security policy that governs information flow between objects

Any information system designed based on information flow is secure if there are no illegal flows.

Though the advantage of information flow models is that they cover all kinds of information flow, it has been observed in practice that such systems are hard to design. It has also been observed that checking if a given information system in information flow model is secure is *an undecidable problem* [43].

3.2.2 Second Phase: Access Control Lists, Role Based Security, Trust Models

This phase is characterized by the increasing use of computers in business with technology innovation that lead to local and wide area networking, desk top computing, and databases. It was also the beginning of the internet. As the level of security awareness and its impact on business was understood, enterprises considered different types of security models and paradigms to manage their information assets. There are

many products and solutions offered by Vendors to deal with enterprise security. This section focuses on the security models based on access control lists, roles, and trust.

Models based on Access Control List (ACLs)

Access Control Lists are a mechanism to implement access control matrices [24]. Strictly speaking these cannot be classified as a security model. Instead, these can be more appropriately termed as mechanisms to implement permissions modeled by an access control matrix. Using a matrix directly has many drawbacks such as the size, space utilization, and poor scalability [44]. Access Control Lists have been used widely in the industry because of their conceptual simplicity. An Access Control List is defined as a collection of pairs including subjects and the rights they have over a specific object or a system resource. It also provides mechanisms to aggregate subjects and objects into groups. The space usage is effective in ACLs because there is no need to maintain all subject-object pairs. The specification of the rights of subjects over objects could be either positive rights (Grant) or negative rights (Deny). In other words, ACLs allow us to maintain both white lists (focus on grant of access) and black lists (focus on denial of access). This makes it possible to specify default rights, thus facilitating further reduction in the size of lists. ACLs have also been discussed in [45] where the authors propose new forms of access control beyond the discretionary and mandatory models.

As Bykova discuses in [44], ACLs have several drawbacks because of the fact that they allow for aggregation and default permissions. Writing the rules could be error prone and also maintaining these rules from a change management viewpoint is tedious and challenging. This is because of the possibility of conflicts and unforeseen rules conflicts.

In spite of its drawbacks, they have been very popular as a security mechanism because using these lists one can specify a large variety of security rules in many different domains. They are widely used in operating systems and network security (firewalls).

Role Based Access Control (RBAC) Models

In the 1990s, these types of models began appearing in the security research community and enterprises have adapted variations of these models to implement their information security strategy [46]. While most of the early models focused on Discretionary Access Control and Mandatory Access Control, the RBAC model [47] gained wider attention in implementation of enterprise security. This is because of its inherent conceptual simplicity in modeling enterprise environments. The foundation of the RBAC model is the notion of a *Role*. A Role is characterized by a set of tasks and permissions are associated with Roles [48]. Users are assigned to Roles based on their responsibilities, thereby acquiring the corresponding permissions and access rights. Users can be reassigned to Roles which can be given new permissions or some of the assigned permissions revoked. As new applications are integrated into an enterprise system, new roles can be added, existing roles can be modified and user-to-role mapping may be modified. Conceptually, the RBAC model provided a foundation well suited for enterprise security management.

Several variations of the RBAC model have been proposed in the literature, each one differs in how role hierarchies and constraints are handled. The model has been extended to include the notion of *time*, called Temporal Role Based Access Control (TRBAC) [49], Generalized Temporal Role Based Access Control (GTRBAC) [50].

RBAC model's acceptance and popularity in the industry can be gauged by the fact that it has been used to implement various access management solutions in a wide spectrum of industry domains such as the health care, financial, network administration, and many more. There is an entire conference, ACM workshop on Role Based Access Control, devoted to stimulating further research and applications of the RBAC model. Though the model is intuitively simpler, one of the disadvantages of implementing access management based on functional roles is the effort involved in configuration and change management of Roles [51]. In a typical enterprise, users belong to multiple hierarchies in an organization. It is not atypical to find more than 20 hierarchies in an organization. For example, in a large enterprise, employees can belong to a HR hierarchy, Sales hierarchy, Functional hierarchy etc. In such a context it becomes a complex administrative process to design, implement, and dynamically manage role based access control mechanisms.

RBAC is very much an active area of research for the many benefits it provides in dealing with enterprise security. The section on collaboration security in this chapter will present further research on adapting RBAC model in the context of collaboration.

Trust Based Models

In the middle of 1990s Decentralized Trust Based Management systems began to appear in the security research community [52]. The principle behind these systems is the idea of negotiating trust between strangers. It relies on two concepts: *security credentials, and security policy*. An owner is authorized to access protected information object (granted trust) if the owner's security credentials satisfy the security policies. The trust based security models research has spawned various branches of research and is

also being used in implementing security solutions in an enterprise. Automated trust negotiation is discussed in the papers by Winsborough in [53] and [54]. Li discusses the idea of discovering credentials in distributed systems for trust management [55]. Protecting credentials in trust negotiations is discussed in [53], and [56]. The idea of adaptive trust negotiation is presented in [57] in the context of electronic business transactions that often take place between entities that are strangers to one another, for example in online communities. In this scenario, establishing trust is more complex because participants belong to different security domains. As discussed in [57], trust management is a key issue in today's environment of internet-enabled e-commerce. The web necessitates decentralized systems that span multiple domains, each one having its own set of security policies. Trust management is a framework for providing decentralized security related decisions. It brings the level of abstraction to the level where the focus is on why trust should be granted in contrast to immediately focusing on security mechanisms such as cryptography, Read | Write | Execute access etc.

As discussed in [58], trust management is based on three basic elements: principles, principals, and policies. *Principles* focus on being certain about what privileges will be granted to a *Principal* who is trusted to take actions on some objects. *Principals* are 1) people, 2) computers, and 3) organizations. The decision to grant trust is justified by a sequence of assertions. All three types of principals stated above make assertions based on their particular identity lifetimes: *people* make assertions with broad scope, bound to their long-lived *names*; *computers* make narrow proofs of correct operation from their limited-scope *addresses*; and *organizations* make assertions about people and computers because they have the widest temporal and legal scope of all.

Credentials describe each kind of principal and its relationships, such as membership and delegation. Policies are rules about which assertions can be combined to yield permission. In essence, policies can grant authority based on the *identity* of the principal asking; the *capability* at issue; or an *object* already in hand. In other words, you might be trusted based on *who you are*, *what you can do*, or *what you have*.

The next section presents some of the new directions in the security research and the associated models. The ideas and concepts presented in these models could be considered innovative though they are not in widespread use in the industry.

3.2.3 New Directions in Security Paradigms and Models

Trust based models are still a relatively young field and are under active development and therefore can certainly be included in this categorization. Nonetheless, the focus of this section is to present some of the other innovative research thoughts and techniques that are proposed to deal with the ever increasing complexity of computing environments and the associated security needs and security management. The professional organization, ACM, introduced the ACM New Security Paradigms Workshop in 1993. Since then, the security research community has been proposing numerous out-of-the-box thinking type security models, mechanisms, and frameworks to deal with security. The purpose of this section is to present several interesting aspects of this research without going into all the details.

As stated earlier in the introduction, security requirements have evolved over time as the computing environment continued to advance and encompass different types of

people, processes, and organizations interconnected through the Internet and Intranet. The concept of a boundary has essentially become a moot point. In such a context the old security models and paradigms do not scale well. They were good and effective for the then intended applications: Military and Government. In today's diverse environment, the old models do not scale and as Blakely [59] points out the lack of scalability of old models:

- Policies do not scale well. They become more complex as systems increase in size and complexity, and policy management becomes a challenging task.
- Achieving strong secrecy is difficult because it depends predominantly on people who are not good at keeping secrets in the first place.
- Achieving system integrity is hard, expensive, and requires trade-offs.

Some of the security research presented here could be considered as potential solutions to the growing security needs in the context of evolving computing paradigms driven by social networking revolution. The paper by Bykova [44] provides the basis for Figure 3.3 which captures the various strategies for addressing security and their discussion.

Figure 3-2: Security Strategies

Security as an inherent property

Application architects and designers are realizing that the right approach to ensuring application security is to make security an integral component of their development process. In other words, security is considered an inherent property of the system in contrast to imposing security after the application is developed. Smetters and Grinter [60] present numerous examples of making security transparent in the design of application. Several Identity Based Encryption mechanisms and tools follow this principle [61]. Some other ideas discussed in the literature on this topic are:

- Increasing data size proportional to its value [59]

- This concept relies on the real life fact that most valuable items are very cumbersome and inconvenient to handle. For example, $1 million in the denomination of $20 bills is rather large, heavy, and cumbersome for one person to carry. Similarly, if we make the digital representation of sensitive data very large, then it is rather not very simple and easy to steal the data.

- Unhelpfulness as a security mechanism
  - Nelson [62] introduces the concept of unhelpfulness as a security mechanism. The emphasis is on controlling the flow and rate of information released to a user as a way of managing security and ensuring compliance with the principle of least privilege. The information in an otherwise classified document or subject area is released intentionally slowly in a very unhelpful manner so as to dissuade the user from accessing. In essence, many levels of restrictions are placed to access more information.

Security based on survivability

This approach brings into its fold the notion of business risk into security management. Lipson and Fisher [63] proposed that enterprises look at security from the perspective of risk management as the goal of security is to protect assets. Enterprise risk management addresses protection of assets. These concepts of asset protection could be leveraged in addressing security as well. They define survivability from two viewpoints: 1) Technical, and 2) Business. The technical aspects of survivability deal with ensuring the continuity of services and information is available in spite of the accidental or non-accidental attacks and threats. The business aspects of survivability emphasize risk analysis and management. Specifically it focuses on the business

mission and objectives when quantifying the potential threats and risk to business. The goal of survivability model is to protect the most important business assets, its business mission, while having some level of tolerance toward failure of non-critical components of the business.

Security based on economics

The proponent of this approach is Blakely [59]. Blakely argued that security tied to monetary value is another effective security management tactic. In his paper, Blakely demonstrates this concept with an example from health care applications domain where one of the information assets is patients' health records. The privacy of these records is tied to economics. When some user wants to access a patient's records, some pre-defined amount of money is transferred from the user's account to the patient's account. If the user is the same as the patient then the money is transferred from his account to his account. If the user happens to be the doctor reviewing the patient's records then the amount he will charge the patient is the same amount of money that is transferred in the first place. In the case where the user who accessed a patient's records is unauthorized to begin with, at least the patient has at least some monetary compensation. The basic idea of security based on economics is to take away something of value from the user and reverse it if the user is determined as legitimate.

The other facet of economics based security is the scheme of incentives and punitive measures. This is a possible approach to thwart social engineering based attacks. Here, users are given some incentives so as not to deviate from intended behavior. These types of security mechanisms are further explored in areas such as making users cautious about their passwords and their protection [64].

Security modeled after human immunology

Researchers working on security have been studying how security defense mechanisms could be modeled much like the immune system of the human body. Somayaji and Hofmeyer [65] argue that natural immune system provide a rich source of inspiration for computer security in the age of internet because it exhibits properties like distributability, diversity, disposability, adaptability, autonomy, dynamic coverage, anomaly detection, multiple layers, identity via behavior, no trusted components, and imperfect detection. Jeff Williams [66] argues that from a security viewpoint, both computers and human exhibit many similarities in terms of architecture, interfaces and communication. The question that these researchers raised is: can computer security people learn from how an immune system comes into play to deal with any kind of sickness of the human body? The human immune system consists of numerous imperfect, unreliable, and open systems, much like the internet driven computing environments. Immune systems are not perfect either and they do make periodic mistakes. Similarly, the computer security people have come to the conclusion that security is not foolproof; it has its own imperfections and there is no such thing as perfect mechanisms and perfect security. The characteristics of the immune systems that show promise and potential in computer security are the following:

- Multiple levels of protection
    - Just like in an immune system, an enterprise information security strategy should adopt multiple levels of protection to safeguard assets. This ensure defense in depth of the larger enterprise system.
- Distributed Control

- The decision making process is decentralized much like the immune system. Security decisions are localized and each subsystem or node is responsible for specific security related tasks.

- Diversity
  - Diversity of systems makes it harder for vulnerabilities to spread from one system to another because a known vulnerability in a system may not be present in another. Diversity could also be achieved by making the protection mechanisms unique.
- Adaptability
  - The security system learns to detect new threats, as well as remembers previously detected threats and applies its knowledge to recognize these threats. Adaptability is a feature that we will address in our research as it forms one of the key components of dynamic security management based on self-organizing maps.
- Disposability
  - The essence of this principle is that no system component is vital and that anything can be replaced just like how a cell is replaced in an immune system.
- Autonomy
  - The basic idea is to give a level of autonomy to individual components of a network to make their own security decisions.
- No trusted components

- This is also one of the guiding principles of software engineering programming principles. In essence, it implies that no object or system should be trusted and everything must be verified.

- Identity via behavior
  - In the immune system identity is also verified through behavior. Traditionally a user's identity in a computing network is determined by possession of a secret key. By tying identity to user's behavioral patterns, security could be enhanced, as the security management tool would protect against unusual user activity. For example, many credit card companies use this feature to enhance security and protect the consumer.

Optimistic security

Povey [67] argues that sometimes the static nature of authorization can cause unexpected risks for users working in a dynamically changing environment. This concept is very useful in dealing with mission critical systems such as natural disaster emergencies and hospital emergencies. In such situations, we have personnel who go beyond their normal duties in order to address unforeseen disasters and emergencies. *Optimistic security model is built on the notion that it is valid to increase the privilege levels for information access dynamically in situations like the above.* The other underlying assumption of this model is a user rarely attempts to access information that they are not privileged to have. It is argued that providing an optimistic scheme alongside a traditional access control mechanism can provide a useful means for users to exceed their normal privileges on the rare occasion that the situation warrants it.

Strike Back security

In this approach, the emphasis is on aggressively targeting the enemy in contrast to the traditional defensive security strategies. When the system detects a cyber-attack, it should aggressively go after the attacker and try to identify the enemy's center of operations and destroy it. This approach is discussed in [68] to deal with cyber security and the increasing importance of the viewpoint that such cyber-attacks are a threat to national security. In such a situation, just passive defense alone would not suffice a path of action should be taken to destroy the enemy. Honey Pots based security mechanisms could also be classified into this category [69]. A honey pot is a computer system on the Internet that is set up for the sole purpose of attracting and trapping people who attempt to penetrate other people's computer systems.

Functional approach to security

Nelson [70] argues that security issues are primarily addressed in the context of the application's intended functionality and needs. Instead of trying to implement security solutions, based on generalized models or formal models, it is important to truly understand what a secret is in the application before the security mechanisms are defined. In other words, the application semantics and the associated data must drive the security decisions. Nelson makes the observation that security cannot be expressed accurately using only syntactic notation. A second observation that Nelson makes is that functional models that address security from application and data perspective capture the required behavior more accurately because they consider the semantics of the application. This approach essentially ties very well with best practices in application development where the requirements drive the design and development of a system.

The focus of the next section is Software Security, which is an emerging branch of security. It deals with the design and development of software systems keeping security in mind. The aim of software security field is to integrate security across the entire software development lifecycle [71]. The section presents an overview of the types of attacks and counter measures that are proposed to thwart such attacks. Any enterprise security framework must integrate the software development process lifecycle into its overall security strategy because many of the security compromises that have been occurring recently and well publicized are the result of poor secure programming practices.

3.2.4 Software Security: Attacks and Counter Measures

Practitioners and Researchers have realized that the root cause for many security compromises lies in the fact that the software has been poorly designed to defend against malicious attacks. In spite of a security strategy that includes hardening the operating system (access control matrices), hardening the network (firewalls, intrusion detection etc.), many security breaches continue to occur and they are traced to design and implementation flaws such as poor error handling design, hard coding secrets in code, not validating inputs for size, not documenting assumptions etc. Integrating security into the full development lifecycle has become such an important issue for practitioners that even large companies such as Cisco and Microsoft have instituted processes, methods, and tools in place to ensure that software security is addresses thoroughly right from the beginning in contrast to addressing it as an afterthought.

In the famous Microsoft memo by Bill Gates [72], he emphasizes the role of software security. In his words, software should be so fundamentally secure that customers do not even have to worry about it. He goes on to say, “when we face a choice between adding features and resolving security issues, we need to choose security.” It has become imperative that we design systems that continue to operate reliably even under the constant barrage of hacker attacks. Figure 3.3 depicts the code base of Windows (up to XP) since Windows NT was first released in the 1993.

Year	Operating System	Lines of Code (million)
1993	Windows NT 3.1	6
1994	Windows NT 3.5	10
1996	Windows NT 4.0	16
2000	Windows 2000	29
2002	Windows XP	40

Figure 3-3: Windows lines of code

(Source: [71])

The sheer size and complexity of the software makes it vulnerable to attacks. Many industry experts have claimed that there is a direct relationship between the number of lines of code and the number of bugs [71]. Figure 3.4 shows the critical vulnerabilities addressed by Microsoft.

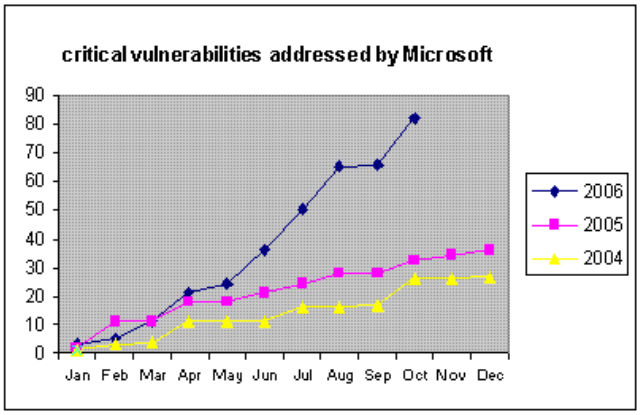


Figure 3-4: Critical vulnerabilities addressed by Microsoft

(Source: McAfee Avert labs Blog, October 11, 2006)

The number of critical vulnerabilities addressed by Microsoft in 2006 is greater than the sum total of vulnerabilities addressed in 2004 and 2005 (note: this research survey includes figures for the evolution up to Windows XP which is still the predominantly used Windows OS. Later versions such Windows 7 and 8 are still not widely implemented in enterprises)

The attacks have evolved from simple password guessing in the 1980s to highly sophisticated attacks such as the Denial of Service, Cross Site Scripting, and Port Scanning. There are several ways to classify the attacks against software systems and in this section they are classified based on the classic CIA (Confidentiality, Integrity, and Availability) model of security [73].

3.2.4.1 Software attacks

Attacks against availability

These types of attacks attempt to overload a system and its resources with the intention of either degrading their responsiveness or making them unavailable for a certain time. An example in this category is the *Denial of Service* (DOS) attacks. A DOS attack is an

explicit attempt by a malicious hacker to prevent legitimate users from accessing system services or cause severe delays in time-critical operations. PING flood or Sync flood attacks are examples of DOS attacks.

Attacks against confidentiality

The aim of these attacks is to expose the contents of communication, or leak sensitive/confidential information of a system. Network sniffing which lets an attacker listen to computer conversations with the help of protocol analyzers is an example of such an attack. Data aggregation attack that allows an attacker to deduce classified information from unclassified information is an attack against confidentiality. For example, a malicious hacker could determine the salary of an employee in a group by looking into information like the group's expenditure before and after hiring the employee. Attackers could also indulge in password sniffing to gain unauthorized access to a system masquerading as a legitimate user and steal/modify sensitive data.

Attacks against integrity

These types of attacks attempt to maliciously modify communication contents and/or data. Man-in-the-Middle attacks are an example in this category. The attacker reads and modifies messages between a sender and a receiver without letting either one know that they have been attacked. Web site defacing and hijacking are examples of this category.

In general, attacks against systems impact multiple security objectives. For example, the payload for Virus attacks targets both confidentiality and system integrity. These payloads can destroy files, reformat hard drive or just degrade performance by

consuming storage space and memory. Unauthorized access attacks where an attacker is able to bypass a weak or ill-designed authorization procedure could impact confidentiality as well as integrity.

3.2.4.2 Countermeasures

Practitioners and Researchers have been designing and developing a variety of countermeasures to deal with the above-mentioned software attacks. These measures increase the security level of software systems. Usually, countermeasures are designed such that they protect against many different type of attacks. These countermeasures span the spectrum of computing environment and address issues at physical layer, network layer, operating systems layer, database system layer, and application layer. Some of the categories of countermeasures include the following:

Authentication

As a countermeasure, authentication plays an important role toward meeting security objectives. This is a process where one object proves its identity to another object. There are two types of authentication that are relevant in a distributed computing environment [74].

- *User-Computer Authentication*

  Authentication accomplished through a combination of techniques like passwords, cryptographic tokens, smart cards, or any biometric features such as face scanning or fingerprints.

- *Authentication in Distributed Computing Environment*

Authentication occurs at multiple places as the user's request is processed at several machines in the network.

Access Control

This refers to the set of mechanisms that allows managers of a system to set parameters, confidentiality restrictions over the behaviors, usage and data content in a system. They can specify what users can do (capabilities), which resources they have access to, and what operations they can perform. Access control has also been called *Authorization*. This is an important facet of software security. A correctly designed access control may help in prevention of attacks such as unauthorized access attacks. Note that access control requires authentication as a prerequisite. When implementing access control management solutions, enterprises first have to define access control policies that provide general guidelines about how access is controlled and how access decisions are determined. There are three commonly discussed access control policies: 1) Mandatory Access Control, 2) Discretionary Access Control, and 3) Role Based Access Control. A complete explanation of these policies can be found in [37]. Numerous mechanisms exist that implement access control policies. These include access control lists, capabilities, and authorization tables [27]. The access control mechanisms facilitate enforcement of security objectives such as availability, integrity, and confidentiality by limiting access.

3.2.5 Most Recent Phase: Social Networking and Cloud Computing Security

The most recent trend in computing evolution is the rapid adoption of social networking, as witnessed by the rapid growth of companies like Facebook, and Twitter. The other trend is the adoption of cloud based service offerings by companies such as Salesforce and Dropbox. Smart phones and mobile applications continue to evolve too. Security continues to be addressed in these areas. This section presents some of the most recent research in social network and cloud computing security.

Social Networking Security

Gao et. al. presents a survey of security issues and available defense mechanisms in online social networks in [75]. They categorize the possible attacks in social networks into 1) privacy breaches, 2) viral marketing, 3) network structural attacks, and 4) malware. As the authors discuss, there is significant personal information shared by users in social networks including their pictures, birth dates, addresses, and phone numbers. This makes it possible for a privacy breach attack because the service providers have access to this information and they in turn could use such data to provide value to their advertisers. The paper suggests the use of user-defined and controlled policies in order to mitigate the leakage of private information. The defense mechanisms include encryption of data and its storage location. The authors present discussion on other categories of attacks as well.

Chris Rose [76] argues that massive over sharing of information in social networks combined with the prevalence of location based information poses greater security risks because the aggregation of all available data will lead to unintended consequences to

users. For example, both Google maps, and Twitter have a feature that when enabled, makes the users' location available when they post data to social networks. This in turn may lead to unintended consequences such as, for example, letting others know that one is not at home etc.

To deal with security issues concerned with social networking, instead of a centralized application based approach to social networking, a prototype of a decentralized, open, and trustworthy social networking architecture, called PrPl (short for Private-Public), is discussed in [77]. PrPl gives the users the ability to keep their data in different administrative domains but makes it possible to interact with each other. Users have a choice and flexibility in services that offer different levels of performance and privacy. For example, the users could store data in personal servers at home, keep it in the cloud based data hosting service provider, or host in a free ad-supported portals. The prototype system provides open APIs for building distributed applications across multiple administrative domains to perform queries and access shared data.

A new perspective on reasoning about security risks in social networking is discussed in [78]. In the paper the authors argue that when a user accepts a new friend in a social network site, the user should ensure that the new friend is not an increased security risk to the entire friend network. The paper discusses different levels of indices to assess vulnerabilities of new friends that guide security based decisions. Each user in a social network has individual as well community based settings. The authors argue that evaluation of these settings guide a user in assessing the vulnerabilities of their friend.

Michael Backes et. al. [79] discuss a cryptographic framework to achieve access control, privacy of social relations, secrecy of resources, and anonymity of users in social networks. They argue that privacy as well as anonymity are important factors for social network security. Esma Aïmeur et. al. [80] identify and discuss three privacy risks in managing social network security. These risks are categorized as 1) security risks, 2) reputation and credibility risks, and 3) profiling risks. Security risks encompass identity theft, phishing, scam, predator and other cybercrimes. Reputation is the social evaluation of public of a person or an entity. If reputation is damaged it impacts the credibility of a user or an organization. Profiling is the recording and classification of behaviors.

The research investigation clearly shows that security in terms of access control, privacy, etc. continues to be addressed in the context of social networking. This subject area is an active area of research from the perspective of engineering, technology, management, economics, and social sciences. Another aspect of technology evolution is the concept of cloud based service offerings. The next section presents a brief review of security literature in cloud computing.

Cloud Computing Security

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [81]. The essential characteristics of cloud computing are: 1) on-demand self-service, 2) resource pooling,

3) broad network access, 4) rapid elasticity, and 5) measured service in terms of metering the usage. In the cloud, there are three service models: 1) software as a service (SaaS), and 2) platform as a service (PaaS), and 3) Infrastructure as a service (IaaS). Finally, a cloud computing environment can be deployed as 1) private, 2) community, 3) public, and 4) hybrid.

Brian Hay [82] discusses the security challenges in the context of providing infrastructure as a service in which units of computations are allocated as virtual machines (VMs) and users access these resources over a wide area network. The new critical parameter in this context is the changing perimeter that extends beyond the the traditional enterprise boundaries and that which is controlled by external entities and users. The security concerns are how to protect the data in transit and in cloud storage, and how to ensure that resources are protected from the service providers. A primary technical challenge is the level of trust accorded to the resource provider. It becomes important to define the levels of operational trusts and to use these levels to perform risk assessments. The author discusses the notions of encrypted communication channels, computation on encrypted data etc. to address security risks.

Wayne Jansen presents guidelines in security and privacy in public cloud computing [83]. The report discusses key security issues in governance, compliance, trust, architecture, identity and access management, data protection and incidence response. A security management framework for collaboration based cloud computing is discussed in [84]. The paper introduces an approach that tackles loss of trust and security control by enabling cloud consumers (CCs) to extend their security management practice (SMP) on their cloud hosted assets. In [85], the author discusses

cloud computing security in terms of possible network attacks. These include distributed denial of service (DDOS), man in the middle, network sniffing, and SQL-injection attacks. In [86], the authors discuss the notion of trust in cloud computing security. From the traditional viewpoint of perimeter security, the cloud appears outside the trust borderline of an organization. If this is viewed with suspicion then it adversely leads to not trusting essential business services available in the cloud. This paper discusses the use of a Trusted Third Party within a cloud environment by enabling trust and using cryptography to ensure the confidentiality, integrity and authenticity of data and communications, while attempting to address specific security vulnerabilities. A detailed analysis of cloud computing security issues and challenges is presented in [87]. The authors discuss the seven security issues that must be addressed in switching to cloud computing model: 1) privileged user access, 2) regulatory compliance, 3) data location, 4) data segregation, 5) recovery, 6) investigative support, and 7) long term viability.

New computing paradigms lead to new ways of working and collaboration which in turn necessitate new models of access management. As a result, access control management continues to be an active area of research as witnessed by the continuing publication of research papers and call for more papers by a variety of conferences that focus on addressing security and privacy. The next section presents a survey of access control management research from the perspective of collaboration characterized by the evolving nature of computing paradigm driven by web 2.0 technologies, social networking paradigms etc.

3.3 Collaboration Security

Collaboration is the act of working with another or others jointly on a project. From a business perspective, collaboration is the act of working together to achieve a business objective. A working definition of collaboration as presented in [88] is:

> "*Collaboration is a mutually beneficial and well-defined relationship entered into by two or more organizations to achieve common goals.*
>
> *The relationship includes a commitment to: a definition of mutual relationship and goals; a jointly developed structure and shared responsibility; mutual authority and accountability for success; and sharing of resources and rewards.*"

It has evolved from collaboration in the small to collaboration in the large [89]. The small vs. large perspective could encompass, people, departmental and organizational boundaries within an enterprise or inter-enterprise and massive collaboration on the internet in cases such as the open systems development where thousands of developers are working on a project. Collaboration has security implications because many people, processes, and organizations work together and share numerous artifacts and resources. It is self-evident that not everyone needs access to every resource or artifact. In addition, there is information that is business sensitive and there must be some mechanism of managing access to sensitive information. So, in essence Collaboration security becomes pertinent and has access control management implications.

Collaboration security has evolved in step with the changing computing paradigms. The simple access control matrices [34] evolved into Role Based access control methods in the 1990s [37] reflecting the new ways of inter-organizational interactions. Advances in

technology further expanded the scope of collaboration to inter-enterprise as well as open systems collaboration on the internet. Collaboration security in the context of healthcare is discussed in [90]. In a hospital, patient information must be shared among a variety of physicians, nurses, insurance administrators etc. They give an example of a medical record of a patient that may contain information about HIV but should not be shared with the cardiologist treating the patient. They discuss the role of a “security mediator” which monitors the access control in such a collaborative environment. This mediator implements the policies set by the enterprise. The use of certificates in f distributed management of access rights is presented in [91]. Every resource has designated stake holders who impose what is known as “use conditions” on the resource. All the use conditions must be met in order to satisfy the requirements for access. A policy engine matches the attributes of a user requesting access to a resource to the use conditions associated with the resource. Only when all use conditions are matched, access is granted.

Caralli and Young [92] discuss a viewpoint that emphasizes process improvement approach to secure collaboration. They argue that the new operational environment consisting of distributed workforce, heightened threat level, increasing criticality of data security and privacy dictate that security must be viewed as an operational risk management activity that serves two purposes: 1) prevent disruption to core business drivers, and 2) sustain the survivability of the organization’s mission.

Pearlman [93] discusses a community based authorization in group collaboration. The premise is that organizations have highly controlled sharing rules. The set of individuals and /or institutions defined by such sharing rules form a virtual organization (VO). Infrastructures that support the creation and operation of these VOs are called Grids. In the context of these Grids, how to specify community policies remains a challenge. The authors argue that instead of specifying these policies statically which poses an administration challenge, resource owners should instead grant access to blocks of resources that they own to the community as a whole, and let the community manage the fine grained access controls within that framework.

Olmedilla [94] presents a discussion on security and trust in semantic grids that allow for sharing of services and resources across institutions. It is argued that existing authentication and authorization mechanisms are rigid and they do not have the ability to determine how trustworthy the results obtained from a specific provider are likely to be. The trust aspects of collaboration are reflected in three questions: 1) Do I (the recipient of service) believe what Provider A says is true and factual? 2) Do I agree with the answer that is provided by a Provider or Group? 3) Do I believe that the goals and/or priorities of a provider/group match mine? The paper also presents related work in policy based and reputation based trust management. In policy based trust management, the access control decisions are based on specification of detailed rules and reasoning based on rules for trust management. The reputation based trust models are used in e-commerce type environments (example: eBay, Amazon) and are gaining acceptance in ad hoc and mobile networks. The key aspect of the reputation trust model is how to model and compute trust.

A survey on trust in computer science and semantic web is presented in [95]. In this paper, it is noted that trust is an essential trait of interaction and it entails uncertainty and risk of negative consequence. In computer science, trust is a widely used term with many different definitions given by researchers in different areas. The semantic web vision, as formulated by Berners-Lee [96] included the notion of trust. As discussed in the paper [95] trust has another important role in the Semantic Web, as agents and automated reasoners need to make trust judgments when alternative sources of information are available. Computers will have the challenge to make judgments in light of the varying quality and truth that these diverse “open” (unedited, uncensored) sources offer. The reader is referred to this paper for a detailed overview of trust in semantic web.

As discussed in [10], in scientific collaboration, resource sharing tends to be dynamic and often ad hoc which necessitates comprehensive and flexible approaches to cope with access control requirements for ad hoc collaboration. The scenario discussed is that of digital information sharing. In order to share, originators publish their original resource in the collaborative community. Resource discovery leads a collaborator to become aware of the availability of the resource. The collaborator must request to share the resource through resource acquisition. The originator sends a copy of the digital resource to the requester and fulfills the initial resource dissemination. With the consent of the resource owner, the resource recipient may further re-disseminate the pre-obtained resource copy to others. The author states that in a collaborative sharing environment, all participants and their capabilities should be clearly defined, and all sharing behaviors should be highly regulated. In order to manage the complexity

involved in dealing with many individual users in a collaborative environment, the paper proposes a role based framework to address distributed access control, delegation, and dissemination control involved in resource sharing.

In [97], the authors discuss access control aspects in enterprise system based on organization models. In today's enterprises, there is increasing number of collaborative processes which necessitates complex security policies within the confines of organization structure. Thy dynamicity of continually evolving software and collaborative processes dictate that organization structures are capable of quickly adapting to changes. In this context, the authors propose adding a fifth requirement to the original list of four basic requirements that a system should have, proposed by Ellis [98], when an accesses control subsystem is to be implemented:

1. The mechanism should be simple.
2. The mechanism must be unobtrusive to users. It should be naturally integrated with the rest of the system. The system modeling should not increase the complexity of the modeling elements.
3. At any moment in the system's life, it should be easy to check authorization for any system resource access.
4. The effects that access control causes on the rest of the system should be clear and easy to understand.
5. Integration of security elements in the models that are used to describe system functionalities

The paper [97] shows how the dynamic aspects of collaborative systems are represented and further shows the adaptability of role based access control model in their system.

In [9], collaborative access control is discussed in the context of growth in enterprise networks where teams span geographies and are located at multiple sites across the world. They discuss three collaborative access control models: 1) Editing model, 2) Space model, and 3) Role based model. In the editing model, users interact with a collaborative application by concurrently editing its data structures. In the space model, the large collaborative environment is divided into small regions that are manageable. Using the concepts of boundaries and access graphs, access control is managed within a region and when crossing boundaries. In the role based access control, a user is given the access control permissions based on the responsibilities associated with the role. In [99], the criteria for evaluating various access control models of collaboration are discussed. These criteria include: complexity of the access control model, understandability, ease of use, and support for collaboration. An access control mechanism based on trust and social networks is discussed in [100]. The paper discusses the concepts of fingerprints in the context of e-professionals working remotely and collaborating with their peers. Finger prints essentially represent the actions of the e-professionals In the process of their work and collaboration. These finger prints provide the necessary clues to extract their social network information. Combining these with contextual information and trust may yield insights to access control policies.

There is active research on access control mechanisms in the context of cloud computing and collaboration as discussed in [101]. In the paper, a case is made that the emergence of grid and cloud computing has introduced new security concepts. As a result new access control approaches are required. The author proposes a four layer

abstract categorization of a grid for defining access control requirements. The paper presents an argument that the existing grid solutions do not have a standard categorization and that makes it difficult to clearly capture access control requirements.

This section has provided insights into active areas of research to address security and trust issues in semantic web, grid computing based organizations, and in general the domain of dynamic collaboration where people and organizations are geographically dispersed, often assembled together in an ad hoc manner to work on a project, and once it is complete disperse. Some of the additional relevant research in access management with emphasis on dynamic collaboration, social networking, and security management standards can be found in [102], [103], [104], [105], [106], [107], and [108]. This research will adapt the appropriate ideas presented in these domains of knowledge while formulating an access control management solution in inter-enterprise collaboration in the context of onboarding. The next section focuses briefly on the concepts of self-organization whose principles and ideas have applicability to this research.

3.4 Self-Organization

Self-organization is defined as the "*Ability of a system to spontaneously arrange its components or elements in a purposeful (non-random) manner, under appropriate conditions but without the help of an external agency*" [109]. It is as if the system knows how to 'do its own thing. Examples in natural sciences include planets and galaxies, cells and organisms in human body. In [110], the authors discuss the necessary conditions under which a system could be called self-organizing. They use the concepts

of “entropy” from thermodynamics, the role of the observer, and the property of “emergence” to describe the characteristics of self-organizing systems.

Self-organization has been applied in the design and implementation of access management solutions in ad hoc networks [111]. The paper presents a self-organized mechanism to control user access in ad hoc networks without requiring any infrastructure or a central administration entity. Node level access management using the concepts of self-organization and trust models is discussed in [112]. In the context of huge amounts of distributed data in pervasive computing, a self-organized multi agent approach for distributed data management is proposed in [113]. Other research papers in using the concepts of self-organization in distributed systems and networks include [114], [115], and [116].

A self-organized system design methodology is discussed in [117]. The methodology consists of five stages to design and develop complex systems: 1) representation – specification of the complex system in terms of components, 2) modeling – specification of adaptive control mechanisms to ensure that system does what it is supposed to do based on requirements 3) simulation - simulate the model to test different scenarios and mediator/adaption strategies, 4) application – develop and implement the system, and 5) evaluation – evaluate the system from the viewpoint of performance, functionality improvements etc. These steps are not sequential but iterative with feedback between the stages. A bio-inspired P2P (Peer-to-Peer) framework for self-organizing distributed systems is discussed in the context of cloud computing in [118]. It presents a discussion on the relationship between peers and the resources through mechanisms based on a

set of binary keys and a ring topology through which peers are connected. The principles of self-organization are explored in the classic paper by Ashby [119] where the author discusses the concepts of organization which includes conditionality between the components, the role of an observer in viewing a system as organized or not, and the role of learning and feedback in self-organizing systems.

The survey on self-organizing systems shows that it has been adapted in domains such as distributed networks and collaboration contexts. This research aims to investigate this concept further in the context of inter-enterprise collaboration security in onboarding.

3.5 Information Security Standards

Standards play an important role in all domains. They enable good practices, streamlined processes, manageability, accountability, governance etc. There are standards for implementing software quality, software development processes, health care, accounting etc. Likewise information security is an area where there are standards. The first and foremost goal of information security is to protect information assets. The security standards include the ISO27K [120] standards and NIST standards [121]. There are many other non-ISO security standards such as the payment card industry (PCI) security standard council which defines standards for enhancing payment card data security. The ISO27K standards are used to plan, implement, certify and operate an information security management system. They also attempt to define the information security related terms and give a comprehensive vocabulary. An updated version of ISO27K security glossary was release at the end of 2012 [120] .

The standards address several aspects of information security. They encompass software development lifecycle and Quality Assurance, systems lifecycle processes, OSI reference model, security frameworks, security management etc. The security aspects addressed include authentication, access control, non-repudiation, integrity, confidentiality, audit trails etc. In addition there are many aspects of network security addressed by these standards. An important aspect of security addressed is the cyber security framework by the NIST organization to reduce cyber risks to critical infrastructure. It consists of standards, guidelines, and best practices to protect critical infrastructure. A draft outline of cyber security framework was release by NIST on July 1, 2013 [122]. Other security standards are defined by organizations such as ANSI, British Standards Institute, COBIT, GAISP etc.

There are in essence a plethora of security standards. From the perspective of this research endeavor, the purpose is not to define an overall security standard. Instead, it is to study one aspect of security, access control management, in onboarding acquisitions. The results of this work may in the future be incorporated in the existing security standards to address mergers and acquisitions.

3.6 Summary

This literature review summarized the evolution of access control management beginning with the first models like the access matrices, access control lists etc., progressing to role based access control, and then to innovations like security based on immunology, honey pots, economics etc. The evolution of computing paradigms, technology innovation, and the advent of internet and web 2.0 brought about different models of computation like the grid computing and the associated collaboration

frameworks. These advances triggered new ideas and thoughts in collaboration security and access control models evolved to those based on statically defined policies integrated with dynamically determined access driven by features like digital certificates, risk management, reputation based trust, authorization delegation, self-organization etc. In the context of this research, a literature review of information security and access management from a historical perspective was published in [123].

The following observations relevant to this research are made from this review:

1. The security research field is still an active area of interest, not only to governments, military and commercial institutions, but also to the common user whose computer is connected to the ubiquitous internet based computing environment, where every computer is a potentially vulnerable target.
2. There is no universally accepted security reference model and framework.
3. Access Control Management continues to evolve with changing technology paradigms such as cloud and grid computing, and changing collaboration paradigms like ad hoc networks, mobile computing. peer-to-peer networking.
4. Role based access control continues to evolve to address new collaboration processes and infrastructures.
5. A combination of organization defined policies and community based trust management is integral to dealing with access control management in collaboration environments spanning both intra-enterprise and inter-enterprise.
6. Change management is not necessarily addressed as integral to new access control management models.

7. Access control management in inter-enterprise collaboration in the context of onboarding is not directly addressed

The current research efforts are positively influencing how access control management is addressed in the current work environment. This research focuses on access control management in inter-enterprise collaboration in the context of onboarding when a company acquires another company. The insights from the literature review like the needs for having a well-defined set of security requirements, the concepts of dynamic collaboration in computing, trust management, and self-organized systems will positively impact this research. The expected outcomes include an access control management model for secure collaboration in boarding along with addressing change management issues.

4 Research Methodology and Research Design

"Research is formalized curiosity. It is poking and prying with a purpose."

-- Zora Neale Hurston

4.1 Introduction

Research is about seeking truth. It is a process of using a variety of methods, tools and techniques to discover new truths and relationships in the world we live in through advanced study. These new truths and relationships further influence how decisions are made to further the goals of an individual, a company, a community, an organization, a country, and the whole world. Research denotes a careful, systematic, insightful, and patient study and investigation in some field of knowledge, undertaken to establish facts or principles. Often, it is a structured enquiry that utilizes well accepted scientific methodology to solve problems and create new knowledge that is generally applicable and useful to solve a variety of problems in the world.

This research specifically is seeking the truth about access control management in inter-enterprise collaboration in the context of mergers and acquisitions where a company acquires another company. The process of integrating and assimilating the acquired company is called onboarding. This is a problem of great interest in today's business environment where mergers and acquisitions are common place for numerous reasons as discussed in Chapter 2 on onboarding. This problem is amenable to further scientific enquiry because of several reasons: 1) the business models of collaboration continue to evolve; 2) current access control management solutions do not adequately address the problem of collaboration security; 3) technology innovation is influencing

new computing paradigms; and 4) inter-enterprise collaboration security in the context of on boarding is not comprehensively explored.

This chapter focuses on the research methodology and design adopted for investigating access control management in inter-enterprise collaboration in the context of onboarding. First, Section 1 presents a philosophical overview of research methodologies in scientific studies. This will provide a perspective on the type of research that is undertaken and the rationale for selecting the methods to explore this research further to arrive at the truth. Second, in Section 2, the details of the research methodology that is adopted for this research is discussed. The section also discusses how the methods adopted facilitate insights into the research problem that this research is attempting to address. Third, in Section 3, details of the research design are presented. Research design is the conceptual structure within which research would be conducted. In the context of this research, it includes the steps that will be undertaken to design the appropriate techniques to collect data from a variety of sources, analyze the data, propose a model, validate the model, and further refine the model.

The terms: methodologies, methods, and techniques are prevalent in the scientific literature. Though these terms are sometimes used interchangeably, it is important to clarify these terms in the context of research.

Methodology

> *A* set *or system of methods, principles, and rules for regulating a given discipline, as in the arts or sciences* [124]
>
> *A system of broad principles or rules from which specific methods or procedures may be derived to interpret or solve different problems within the scope of a particular discipline* [125]
>
> *A* system *of* ways *of doing,* teaching*, or* studying *something* [126]

Method

An established, habitual, logical, or prescribed practice or systematic process of achieving certain ends with accuracy and efficiency, usually in an ordered sequence of fixed steps [127]

A procedure, technique, or way of doing something, especially in accordance with a definite plan [128]

A particular way of doing something [129]

Technique

A way of doing an activity that needs skill [130]

The body of specialized procedures and methods used in any specific field, especially in an area of applied science [131]

A systematic procedure, formula, or routine by which a task is accomplished [132]

Figure 4.1 captures the relationship between methodologies, methods, and techniques.

Figure 4-1: Association between methodology, method, and technique

The terms research methodology and research methods are clarified next.

Research Methodology

The process used to collect information and data for the purpose of making business decisions. The methodology may include publication research, interviews, surveys and other research techniques, and could include both present and historical information [133]

"A systematic way to solve a problem. It is a science of studying how research is to be carried out. Essentially, the procedures by which researchers go about their work of describing, explaining and predicting phenomena are called research methodology. It is also defined as the study of methods by which knowledge is gained. Its aim is to give the work plan of research." [134]

Research Method

> *"Procedures, schemes, tools, and techniques used for various activities in the process of conducting research. They include theoretical procedures, experimental studies, numerical schemes, statistical approaches, etc. Research methods help us collect samples, data and find a solution to a problem."* [134]

It could be observed that from the perspective of research, the research methodology is a collection of steps taken and specific methods used to arrive at a solution.

The term *Research* itself is defined in many ways [135]. The common theme that runs across these definitions is that research is a systematic quest for undiscovered knowledge. It is usually planned, organized, and has a specific goal. However, as the author states, in the strictest sense research can be pursued for the sake of knowledge without a specific goal or a problem to solve. A classic example of this type of research is exemplified by the work of Marie Curie whose research focused on studying the phenomenon of radioactivity. Irrespective of the type of research endeavor (goal oriented, problem solving etc.) the essential aspects of the research undertaking include observations, theorization, experiments, research surveys, arriving at new conclusions and results, reporting, and sharing knowledge. R*esearch* is classified and differentiated in many ways in the literature. Figure 4.2 shows a snapshot of types of research discussed in the literature [136].

Figure 4-2: Types of research

Table 4.1 describes the essential characteristics of these types of research. The table includes two additional research types: mixed methods, and pragmatic in addition to the generally known research types shown in Figure 4.2.

Table 4-1: Characteristics of research types

Research Type	Characteristics	Comments
Basic	Improve knowledge generally without any application in mind [137]. Basic research can be quantitative and/or qualitative	Natural Sciences research in the last few centuries exemplifies this type of research
Applied	Designed from the start to apply its findings to a particular situation [137]. Applied research can be quantitative and/or qualitative	Study of applications of uranium to make atom bomb in 1945 is an example. Most research studies in computer science and engineering exemplify this approach
Quantitative	The emphasis is on observing, collecting and analyzing numerical data [138]; it concentrates on measuring the scale, range, frequency etc. of phenomena	Also known as traditional, positivist, experimental, or empiricist [139]. Use statistical analysis tools for large quantities of data.

	[137].	Classified further into: inferential, experimental, and simulation
Qualitative	Subjective in nature than quantitative research and involves examining and reflecting on the less tangible aspects of a research subject, e.g. values, attitudes, perceptions [137]; collects non-numerical data; Collection and analysis of textual data like surveys, interviews, focus groups etc. [140].	Also known as phenomenological, subjectivist, humanistic, or interpretative [139] Often combined with quantitative analysis in terms of data collection and analysis.
Descriptive	Fact finding inquiries and surveys of what is and what has happened; describes a phenomenon; researcher has no control over variables as in analytical [136]; relies on researcher's observation as a way to gather/collect data [141].	Also known as *Ex post facto* research in business and social science research [136]. Quantitative techniques are most often used to collect and analyze the data for reporting.
Analytical	Critical thinking to find out facts about a given topic. After evaluation of facts, the answers drive the activities of proposing new ways of addressing the topic. Facts and data drive critical evaluation [136];	Clearly defined topic helps in analytical research. Involves exploration and evaluation.
Conceptual	Related to abstract ideas or theory. Used to develop new concepts or re-interpret existing ideas [136].	Often used by formal thinkers and philosophers. Focuses on developing a theory to explain behaviors and phenomena
Empirical	Emphasis is on observation and experience of researcher. Data gathered to set up hypothesis and conduct experiment [136]	Useful in contexts where it has to be shown that controlling some variable leads to meeting certain objectives
Mixed Methods	Combination of approaches including quantitative and qualitative approaches [142]	Most of today's research is based on mixed methods

Pragmatic	Focus is on “what” and “how to” research based on desired consequences [139]. Individual researchers are free to choose the methods, techniques, and procedures of research that best meet their needs and purpose [139]	Pragmatism justifies the methodology of using a combination of research methods as exemplified by mixed methods. Implies different forms of data collection and analysis

The subject area of research types, methodologies and techniques is an active research in itself. The notions of ontology, epistemology, axiology, rhetoric, and methodology are considered in discussing the many ways of understanding and classifying research paradigms and the associated methodologies. Detailed insight into these topics are covered in [139], and [141]. The next section details of the research methodology adopted for this research.

4.2 Adopted Research Methodology

In order to put the adopted research methodology in perspective, the relevant aspects of this research are presented. First, the researcher’s background is presented. Second, the characteristics of the problem are discussed. Third, the research objectives and the research questions are discussed. These will provide insights into the appropriate research methodologies selected to further enable this research.

4.2.1 Researcher’s Background

One of the factors in choosing the research methodology was influenced by the experience of the researcher in the chosen subject area. Both analytical and pragmatic

research methodologies imply this characteristic. The industry background of the researcher is in the fields of information security, change management, Mergers & Acquisitions (M &A) onboarding, and product and application development including IT integration. The experience includes analysis, design, and development of role based access control systems for financial reporting, facilitating partner onboarding integration activities in the context of M&A, development and knowledge sharing in integrating software security across product development lifecycle and facilitating collaboration activities in the context of implementing enterprise solutions. This firsthand experience provides practical insights into numerous aspects of collaboration processes and access control management. Additionally, the experience suggests that there is potential for further investigation to improve the access control management in inter-enterprise collaboration.

4.2.2 Characteristics of the problem

The context of this research is Mergers and Acquisitions (M&A) and more specifically it is onboarding acquired companies. In M&As, when a company acquires another company, there is inter-enterprise collaboration between the companies involved. The nature of collaboration in the context of acquisitions is such that the people who come together to manage the acquisition and onboarding come from different functional units, different organizations, and they have different processes, methods, and tools that they use. Figure 4.3 depicts inter-enterprise collaboration in onboarding acquired companies. The figure illustrates the following:

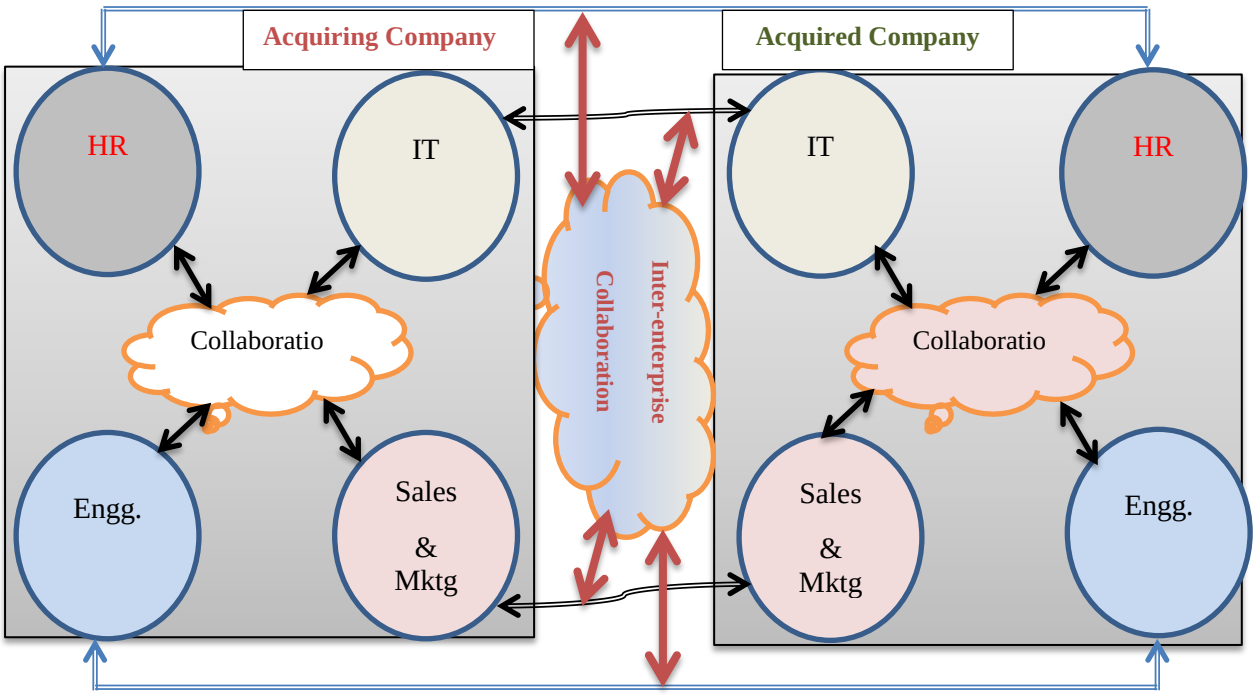


Figure 4-3: Inter-enterprise collaboration

1. There are different functional groups in the acquiring as well as the acquired company, depicted as circles with the names like HR, IT etc.
2. In each of these companies; there is collaboration between the groups t**hr**ough their own collaboration space that may include many different types of collaboration processes, methods and tools. This is depicted by the double arrows going from the circle to the collaboration cloud.
3. In the process of onboarding there is inter-enterprise collaboration among the respective functional groups in the acquiring and the acquired companies. For example, in the Figure 4.3, this is depicted by the double arrows going from HR group in the acquiring company to the HR group in the acquired company. Likewise, the Figure 4.3 shows double arrows going between the other functional groups respectively.

4. The Figure 4.3 depicts the inter-enterprise collaboration cloud; it further reflects this aspect by depicting double arrows from the arrows that denoted such collaboration (point 3 above). In addition, the figure also illustrates that this type of collaboration uses a logically separate collaboration cloud that includes people, processes etc. from both the acquiring as well as the acquired company.

In this scenario, an important consideration is the aspect of security because many business sensitive documents, processes and other artifacts are shared among collaboration teams belonging to different organizations. For example, the collaboration space may include product roadmaps, intellectual property, sales pipeline, customer lists, financial documents, strategic marketing documents etc. This scenario warrants access control management so that it is ensured there is no unauthorized and unwarranted access to information in the inter-enterprise collaboration space. This research is focused on studying the access control management aspects of such inter-enterprise collaboration.

4.2.3 Research Issues

Key findings from the literature review include: 1) access control management continues to evolve with changing technology paradigms, 2) role based access control continues to evolve to address new collaboration processes and infrastructures, 3) a combination of organization defined policies and community based trust management is integral to dealing with access control management in collaboration environments spanning both intra-enterprise and inter-enterprise 4) change management is not necessarily

addressed as integral to new access control management models, and 5) access control management in inter-enterprise collaboration in the context of onboarding is not directly addressed.

This research will leverage insights from the literature review like the need for having a well-defined set of security requirements, dynamic collaboration, trust management, and self-organized systems.

4.2.4 Research Question

Generally, all research begins with a question or questions derived from a general topic that a researcher is interested in. This interest in topic may be due to numerous reasons like the researcher's academic or industry experience, exposure to new fields through lectures and attending conferences, discussions with peers, inter-disciplinary collaboration etc. The desirable attributes of a good research question as discussed in [143] are the following:

1) Relevant

   The question must be relevant in the context of the research topic selected.

2) Interesting

   The topic selected must be interesting to the researcher so that there is self-motivation to investigate the topic and the question.

3) Focused and Specific

   The question must be narrow enough to show focus with potential for specific outcomes. However, to begin with, it can start from a broad topic and narrowed down through criteria like a specific aspect of the topic, a time period, an event, geography, gender, culture, age group, industry etc.

4) Researchable

The topic and the research question must be such that the researcher has access to relevant literature like journals, conference proceedings, technical reports etc. in order to understand what has been accomplished, the progress of the field based on technology advances and paradigm shifts, the still unanswered questions, the gaps in the solutions, and potential for further contribution to theory and practice. In addition, depending on the topic, the researcher must have access to industry practitioners as well to understand the research topic and questions from a practical perspective.

In essence, a research question investigates a specific component of a broader topic area. As discussed in [144], it is a formal statement of the goal of study. It will clearly imply what the study will investigate or attempt to solve. As the author says, the research question is a logical statement that progresses from what is known or believed to be true (as determined by literature review) to that is unknown and requires validation. In the paper by Lipowski [145], a research question is defined as one that is narrow and challenging addressing an issue, a problem, or a controversy. This question is then answered with a conclusion based on further analysis and interpretation of evidence.

4.2.5 Research Question -- Details

The main question that this research is addressing is:

- How can access control in inter-enterprise collaboration in onboarding be improved?

A sub-question that this research is addressing is:

- How can change in administering access control management be managed?

Figure 4.4 depicts the flow in terms of arriving at this question from the broad research topic:

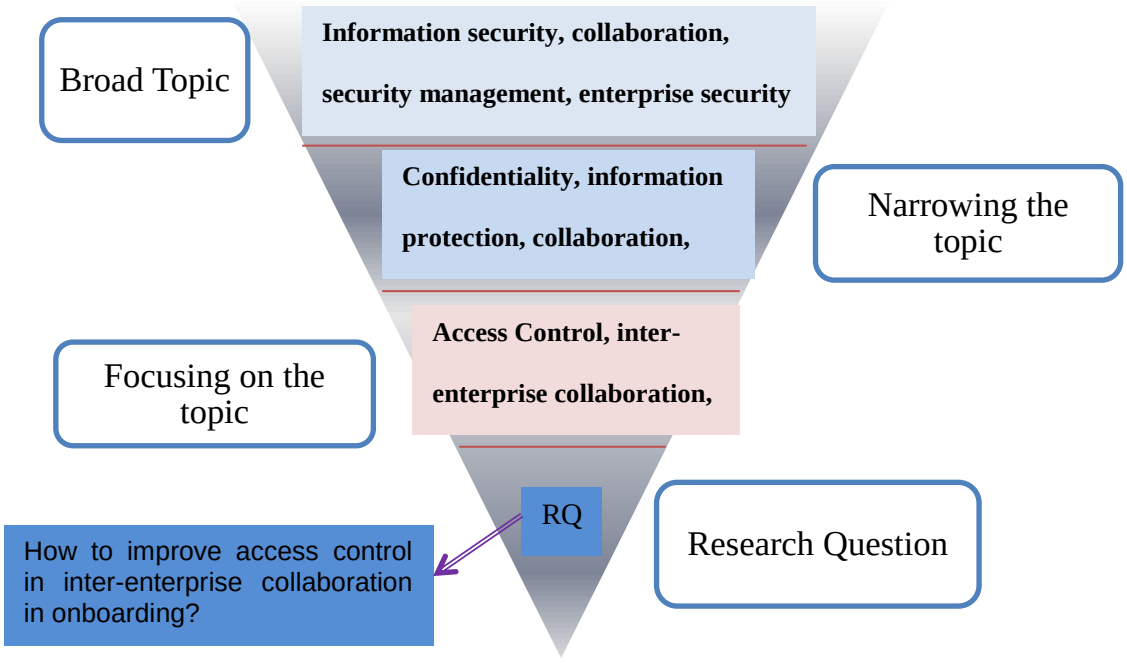


Figure 4-4: The research question funnel

Applying the four desirable attributes of a good research question, as discussed in the beginning of this section, the question is relevant in the context of the broad research topic of information security as confidentiality and protect of information is of paramount importance for a business; the question is interesting to the researcher based on his background, experience, and accomplishments in this subject area, the question is focused and specific because it's goal is to study only the access control aspect of security further narrowing the scope to inter-enterprise collaboration in onboarding; and

it is researchable as demonstrated by the extensive literature review conducted. Finally the question meets the criteria as discussed in [144] and [145] because it attempts to investigate and solve a problem.

4.2.6 Selection of Research Methodology

This research can be classified as *applied research* to begin with based on the criteria presented in [137] which says that applied research focus is to apply its findings to a particular situation. In the case of this research its findings will be applicable in the situation of inter-enterprise collaboration in onboarding. Further, this research can also be classified as *Action Research*. Action research is a form of applied research where the researcher attempts to develop results or a solution that is of practical value to the people with whom the researcher is working, and at the same time developing theoretical knowledge. Action research is discussed in [137], and [134]. This research has characteristics of both *qualitative* and *descriptive* methodologies as well. It is descriptive because it describes systematically the scenario and context of onboarding and the associated problems; while it is qualitative because it collects non-numeric data through surveys and interviews of small number of people, and further asks research question based on “how to”, “why”, “what” etc. This research also uses elements of analytical methodology because there is an aspect of critical thinking about the problem as the researcher participated in onboarding activities and made observations. Aspects of the pragmatic methodology are present in this research as it asks questions such as “how to” and “what” in investigating the topic further. The quantitative aspects of this research encompass data collected through survey which is subject to further analysis. In essence, this research is truly based on mixed methods research methodology where

it relies at the outset on applied, qualitative and analytical approaches supported by aspects of quantitative and action research methodologies.

The mixed methods research methodology applicable to this research further provided insights into the methods used to proceed in terms of data collection and analysis. The action research influenced the selection of experiential project observations to documenting the relevant security issues observed in projects; the qualitative nature of the methodologolgy influenced the selection of expert interviews with M&A experts to gather the relevant field data; and both the qualitative and analytical aspect of this research influenced the selection of a survey design and its administration to the relevant industry and academic experts to gather substantial field data which is further subject to quantitative analysis. The next section provides further details of the overall research design.

4.3 Research Design

Research design is the conceptual structure within which research is conducted. The function of research design is to provide for the collection of relevant information with minimal expenditure of effort, time and money [136]. As discussed in the paper, the preparation of research design, appropriate for a particular research problem, involves the consideration of the following: 1) objectives of the research study, 2) method of data collection to be adopted, 3) source of information—sample design, 4) tool for data collection, and 5) data analysis. Figure 4.5 shows the overall process of this research undertaking.

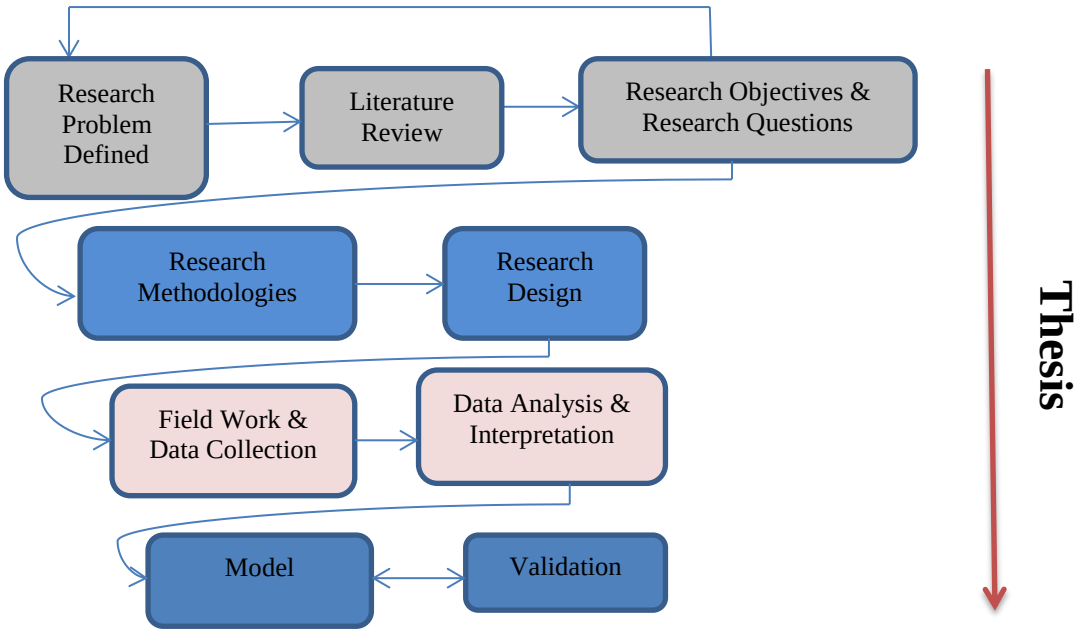


Figure 4-5: Research process

It should be noted that Fig. 4-5 depicts a process flow, numerous activities within the process overlap and not necessarily executed in a strict sequential order. Iniatially, the general problem statement is defined. A preliminary research survey resulted in refining the research problem and research objectives. In the next phase, an extensive literature survey produced in depth secondary data that facilitated further refinement of research objectives based on the gaps found in the literature and insights about potentially leveraging and adapting some of the techniques from subject areas such as self organizing systems. The research methodology and research design phase enabled clarification of the research methodologies applicable for this research and the various tools and techniques that will be used in the phase of field work and data collection, and data analysis and intrepretation. The results from this phase will provide the basis for model development which would further be validated and refined accordingly. The final

step is the completion of dissertation. The field work details are presented next, followed by a discussion on some consideration for model development.

4.3.1 Field Work, Data Collection, Analysis and Interpretation

Experiential observations, expert interviews with Mergers and Acquistions specialists, and administration of a questionnaire on collaboration security form the basis for data collection. The purpose of the survey is two fold:

1. Understand and assess the process of on boarding acquired companies
2. Understand and assess the access control management in inter-enterprise collaboration

A preliminary survey form, shown in Appendix A, was designed and tested with six people who are industry experts in M&A, IT experts and business stakeholders who participated in onboarding activities, and academic researchers with experience in design of surveys. The feedback sought included: 1) the structure and organization of the questionnaire, 2) content relevance and completeness, and 3) clarity of the questions. The feedback enabled the design of an updated questinnaire, shown in Appendix B, that was adminsitered to 25 people in the industry. The experience and background of the survey particpantse includes M&A specialization, Marketing and Sales, Learning and Development, Channel Support, Business Architect, and IT. The survey questinnaire was designed and administered using Google online survey tools. It was mailed to the participants using the tool. The participants received a link to the questionnaire. They clicked on the link and filled out the survey. The submitted responses were automaticlaly gathered by the Google online survey tool. Chapter 5

presents the details of the data collection, analysis, and interpretaion of survey results. The rationale for survey questionnaire design is discussed in the next section.

4.4 Survey Questionnaire Design

Designing the questionnaire right is a critical first step in collecting relevant data for research. The key objective of a questionnaire is getting a complete set of accurate answers which is representative of the population being sampled [146]. There are two types of questionnaires: 1) direct questionnaires are completed by interviewers in face-to-face (or teleconference) contact with the respondents and 2) mail questionnaires are completed by the respondents themselves in their own time, typically administered using online survey tools available in modern times. Unless the number of respondents is relatively small, the cost overhead of direct questionnaires puts them beyond the scope of most projects. In this research online survey mechanisms were used to gather the data after the pilot phase. In the pilot phase, in addition to administering the online survey, a few telephone interviews were conducted to gain insights into the survey questionnaire design and to remove any ambiguities before the survey was sent to participants at large. As discussed in [146], a mail or online administered survey questionnaire are vulnerable in following ways:

1. The questions must be straightforward and easily understood as they stand, since there will be no opportunity to elaborate when the respondent reads the questionnaire.
2. The answers have to be accepted as they stand since there will be little opportunity to seek clarification or to probe further unless this procedure is added to the process.

3. Respondents fill out questionnaires in their own time and can spend as much time as they want in considering their responses. This means that answers cannot be guaranteed to be spontaneous or independent.
4. The identity of the respondent cannot be guaranteed. The questionnaire may state that it is to be filled in by the project manager but there is nothing to stop him or her from 'delegating' this task to a secretary or a trainee.
5. Questionnaires are filled in by those who want to fill them in and avoided by those who don't. Since these groups are self-selecting, an incomplete set of responses introduces bias into the sample, and since nothing may be known about the non-respondents, except that they didn't respond, it is not possible to compensate for this bias, so the best strategy is to try to minimize it by considering ways of improving the response rate.

An important aspect of questionnaire design is that its purpose must be clearly stated at the beginning so that the respondents will know the researcher's objectives of administering the survey. In addition, the respondents sample must be relevant to the survey being administered. The goal of questionnaire design is to frame the questions that meet the following criteria:

1. Can the respondent understand the question?
2. Can the respondent answer the question?
3. Can the designer (or the *surveyor*) understand the answer?

The answers sought by the researcher to survey questions fall under the following categories:

1. Open Questions.

   These are questions which invite a written answer. The respondents can say anything they like. The problem lies in comparing and combining what different respondents are saying since all the answers must be read and interpreted by the surveyor. Surveys frequently present the results of such questions by means of a few well-chosen 'typical' and/or 'extreme' quotations. This is necessarily subjective and qualitative. However, there is scope for some open questions in any questionnaire. The respondents are being asked to think deeply about subjects which may arouse their passions and it may be better to give them an opportunity to vent their feelings in writing rather than tearing up the questionnaire.

2. Coded Questions

   These are open questions to the answers of which the surveyor applies some sort of coding once the questionnaires have been returned. This helps to make the interpretation of answers more systematic and may allow for some quantitative analysis.

3. Pre-coded Questions

   By far the most popular form of questionnaire question is the familiar multiple-choice question. These are useful both for soliciting comparable answers and for easy analysis.

A good practice in conducting surveys is that the initial draft of a survey questionnaire should be piloted to check for ambiguities and mistakes. The pilot will provide insights into making the necessary modifications before the final survey is administered. This

practice has been followed in this research where a pilot questionnaire and its administration led to further refinement in the subsequent survey questionnaire. The next section discusses the steps taken in model development and validation.

4.5 Model Development and Validation

Multiple factors influence the development of the model though the essential elements address the primary purpose of access control management in inter-enterprise collaboration in the context of onboarding. development of the model. Both the literature review and survey analysis provided insights into factors that should be considered in model development:

- Factors from literature review that contributed are:
  - Importance of security requirements
  - Collaborative sharing patterns
  - Trust management
  - Access control models
  - Self-organization in dynamic collaboration
  - Business process of Mergers and Acquisitions

- Factors gathered from survey are:
  - Security requirements must be stated upfront
  - Collaboration onboarding process lifecycle
  - Security in managing onboarding
  - Formation of integration teams in the lifecycle
  - Enterprise Roles in access control
  - Governance and static access control policies
  - Change management

These factors are discussed in detail in Chapter 6 which focuses on model development.

4.6 Summary

This thesis is based on both primary and secondary research. Primary research typifies first hand observation and investigation of the subject; in this case the researcher's experience and observations at workplace influenced the research. In this context, interviews and surveys are also influencing factors in the development of the appropriate access control model for inter-enterprise collaboration in onboarding. The secondary research examined the studies and literature on access control management, collaboration security, process of onboarding, self-organizing systems, and mergers and acquisitions. This chapter provided insights into the philosophy of scientific research and further discussed the various research methodologies and their characteristics. The section on the adopted research methodology presented the research problem in context and discussed the rationale for the mixed research methodology adopted for this research. The section on Research design presented a conceptual overview of the overall research process steps relevant to this study. Furthermore, this section discussed the survey questionnaire that this research used to collect the relevant data from the industry for analysis and interpretation. The section on model development and validation included the research considerations that are relevant in the development of the model.

5 Data Collection and Analysis

"It is a capital mistake to theorize before one has data." – Sherlock Homes

5.1 Introduction

While the literature review provides rich sources of secondary data for pursuing research, it is equally important to identify sources of primary data which provide first-hand information to the researcher. Together, the primary and secondary data provide insights, direction, and a well-defined path to conduct research and contribute to both practice and theory of the chosen research domain. This research has collected data from:

1) Field studies comprising of two experiential projects from the researcher's direct participation and observations in onboarding collaboration for two cross-functional projects;
2) Field studies comprising of interviews with two senior industry experts who facilitated mergers and acquisitions;
3) Pilot survey design and administration;
4) Modified survey design and administration.

The rest of the chapter is structured as follows. First, the field studies data from experiential observations is presented. Second, the field studies data from interviews with industry experts is presented. Third, the pilot survey administration and the subsequent survey questionnaire design update are discussed. Fourth, the final survey administration is discussed. In this context, the profile of the companies and participants

is presented. Fifth, the data analysis from the survey is presented. Finally, the insights gained from the data analysis are presented along with the specific research issues that are addressed in the proposed model.

5.2 Field Studies

This section will present experiential data as well as through the interviews with industry experts in mergers and acquisitions (M&A). Together, they provide insights into the research issues addressed by the model.

5.2.1 Experiential Project 1

This researcher has participated in cross-functional and inter-enterprise initiatives in the high tech industry where his leadership and facilitation experience spans over 25 years in software development, change management, designing security solutions and access control models, leading the development of collaborative knowledge sharing environments, and conducting secure product development training worldwide. The focus of the field study discussed here is an onboarding initiative of a large high tech company in San Jose California which acquired a medium sized high tech company which is based in Europe.

Researcher's Role: Training Process Lead

Responsibilities: Some of the key responsibilities included the following:

- Worked with cross functional teams to understand the acquired company's partner management tools;

- Analyzed and mapped the acquired company's partner management tools and acquiring company's partner management tools (which ran into more than 30 tools);
- Created a plan to integrate tools and training processes;
- Developed e-learning content on top 20 tools and processes.

Company Profiles:

- **Acquiring Company**

  The company is in the business of providing networking hardware and software. They are a fortune 50 company in the world with over 50,000 employees worldwide. Besides the networking hardware and software, the company also sells multimedia virtual conferencing and collaboration solutions and is a market leader in virtual conferencing. The company's business growth strategy includes acquisitions at regular intervals. The acquisitions over the last 10 years included very small private companies of less than 10 employees to medium to large companies of up to 1000 people or more.

- **Acquired Company**

  The acquired company in this case is a global leader in video communications based in Europe, with over a thousand employees worldwide. It was a publicly trading company. They were acquired for over $3 billion. The motivation for the acquiring company is to become a market leader in the field of collaboration which was expected to be over $35 billion in the coming years.

The acquisition legally closed in the second quarter of the year 2010. The process of onboarding collaboration started just before the legal closure.

Onboarding Process

At the highest level there is a corporate development integration team which initiates acquisitions. Some of the cross functional teams collaborating during onboarding were:

- Business Architecture team – responsible for integrating business processes of the acquired and acquiring companies. These processes included sales, customer support, partner support etc.;
- HR team – responsible for onboarding the acquired company's employees which included role mapping, assigning employees to the respective organizations, creating new organizational structures etc.;
- Partner Onboarding team – responsible for mapping the acquired company's partners to the multi-tiered partner and distributor structures of the acquiring company;
- Product Integration team – responsible for mapping and integrating products of the acquiring and the acquired company and assigning these product development streams to the respective product engineering business unit;
- Sales Process integration team – responsible for onboarding the acquired company's sales channel partners and creating the necessary accounts on sales enablement tools of the acquiring company;
- IT Integration team – responsible for mapping and integrating the IT processes that enable business.

During the onboarding process, the cross functional teams had access to a central collaboration repository which was organized by individual teams as well as a globally accessible repository which contained information assets accessible by all teams. Each team put their information assets in the repository. There was an overall project management office and each team had their respective project plans. The structure of the repository itself was not pre-determined and it changed during the course of onboarding.

Onboarding Challenges:

- Delays in project timelines and deliverables;
- Partner onboarding was not smooth because the partner account manager did not clearly understand their roles and responsibilities;
- Partners had access to sensitive information as there was no well-defined process to protect intellectual property;
- There was no well-defined overall onboarding process that everyone got trained on at the beginning of onboarding lifecycle;
- Teams had access to many documents in the repository beyond their scope of work and beyond the completion of the process.

5.2.2 Experiential Project 2

Researcher's Role: Post-Integration Analysis and Training facilitation on behalf of the business architecture team.

Responsibilities: Some of the key responsibilities included the following:

- Analyzed Acquisition process lifecycle for possible improvements;
- Enhanced system and partner onboarding processes;
- Created a plan to integrate partner support which included enhancing the role of partner account managers;
- Created training process for partner onboarding in acquisitions.

There was a central repository accessible to all members of the team with no access control enforced. The onboarding challenges provided a starting point for this project. The team itself comprised of members from more than three different functional organizations including members from the acquired company. The process

improvement suggestions were submitted to the corporate development integration team.

Current Status

The process of acquisition integration continues to evolve. Currently the relevant phases from the perspective of this research are the following:

- Integration engagement and early discovery
  This phase starts during due diligence before the deal is officially closed. High level executive sponsors are briefed and preliminary integration strategy drafts prepared.
- Integration Planning
  This phase starts just before the deal is legally closed. Integration kick-off meeting is conducted, various work streams are identified, detailed analysis and discovery sessions are conducted, detailed data analysis is performed, operational blueprint is defined, project plans are developed, day 1 + 90 day execution plan is created, and integration exit criteria are identified.
- Integration Execution
  Multiple collaboration teams in all work streams work on integration. Employees, customers, partners, products, business processes etc. are integrated. Integration reviews carried out periodically, integration plans updated, work stream project plans reviewed and updated. Feedback from customers, partners, and employees collected, and project is closed out.

The onboarding process comprises of over sixty steps so far and is still work in progress. The number of work streams, where each work stream is a cross-functional team responsible for executing one aspect of integration is over twenty; the number of participants is over hundred, and almost all functional units, such as HR, Engineering,

Sales, Technical Support, Marketing, Partner Support, and Training are involved in the onboarding effort.

5.2.3 Key Insights and Observations from Experiential Projects

This acquisition onboarding undertaking was accomplished over a period of almost eighteen months. It provided numerous inter-enterprise experiences and insights during its lifecycle. The key insights and observations made are the following:

1. The onboarding process is a complex undertaking with multiple teams working on different aspects of integration.
2. Project Management at multiple levels is a critical component of the entire process and it is a challenge to reconcile the dependencies, deliverables and timelines across multiple work streams.
3. The process itself was not structured and well-defined at the beginning and it evolved as the integration progressed.
4. New work streams were identified, existing work streams modified, and some terminated along the process lifecycle.
5. The project closure was delayed by almost six months and budgets were negatively impacted upon.
6. There was no integrated security strategy in place to guide access control management decisions.
7. People had access to business sensitive information assets though their role did not entail such access.
8. Roles and responsibilities were not clearly defined for everyone and often times, these were assigned in an ad hoc manner.
9. Team members cited deficiencies in communication, coordination, and cooperation.
10. There was no well-defined closure at the collaboration team levels and team members had access to sensitive information even after their participation ended.

For example, the access control and security challenges identified by one cross-functional team included the following: (note: the acquiring company is replaced by XYZ to maintain confidentiality.)

1. The lack of screening at registration allows competitor employees to register at XYZ.com and direct competitors to register as channel partners resulting in overt competitive intelligence gathering and theft of XYZ's intellectual property.
2. The lack of centralized user access content management for XYZ.com results in intellectual property leakage, increasing the risk for competitive advantage abuse.
3. Lack of standardization across published content results in an unknown amount of improperly entitled content, increasing the risk for content to be leveraged for competitive advantage
4. Without consistent governance, IP loss/abuse is not tracked, measured or monitored within or across all tiered levels at XYZ.com

An actual log entry from the onboarding project is shown in Appendix A. From the perspective of this research, it is clear from these insights that access control in onboarding is an area that needs to be investigated further. In addition, there is scope for defining an onboarding process lifecycle for collaborating teams where security is built into the entire collaboration lifecycle beginning with the team formation until the team is dissolved and the data archived.

5.2.4 Interview with an Industry Expert in M&A

The interview was conducted with the principal founder of a consulting group which facilitates M&A. The founder has worked in team leadership roles in numerous companies managing acquisitions onboarding before he started his own M&A facilitation company. The essence of the interview is as follows:

1. What is your name? – left out for confidentiality
2. Where do you work? – company name left out for confidentiality
    - *I am the founder of a company that facilitates mergers and acquisitions*
3. How much experience do you have in M&A?
    - *Over 20 years*
4. What is your role in the acquisition process?
    - *Team Leader*
5. Did you consider access control mechanisms in onboarding collaboration?
    - *Yes*
6. Please explain how you handled access control management
    - *Access control was set up after the initial due diligence*
    - *The concept of virtual data rooms was established*
    - *The data was classified by department such as financial data, sales data, product data etc.*
7. What tools did you use to manage access?
    - *I used a variety of environments based on what a client has. One tool that I used is SharePoint where I statically defined access control*
8. How did you manage access to the target company?
    - *The target company had limited access to virtual data rooms*
    - *DRM (Digital Rights Management) was put in place to control the actions that can be performed on files accessed. For example, print capability was disabled in some cases when I deemed it necessary.*
9. At what level did you specify access control?
    - *I set it up at the folder level; data come sporadically.*
    - *When someone uploads files, they inform me and I will take care of setting the access rights to files.*

10. How do you know if someone leaves a target/acquired company or the acquiring company?
    - *When I am informed by the responsible people, I go change the access control accordingly.*
11. When someone requests access via email what actions do you take?
    - *Usually I grant them access to Folder level only so that they can see the folder and get some information about the information contents of the folder. If they need access to the actual information then I get another request for them and I take the appropriate action.*
12. Was the acquisition onboarding process on the projects that you worked on well-defined?
    - *It has not been well-defined and so it was not repeatable. I came up with a manual to make this process repeatable that I use for client engagements*
13. When does integration start in your expert opinion?
    - *Integration starts before the deal closes.*
    - *Due diligence is a step where the acquiring company and the acquired company work together in small team. Integration is part of due diligence process.*
14. What teams are involved in acquisition onboarding?
    - *HR, IT, Finance, Sales, etc.*
15. What is the length of time for completing acquisitions onboarding?
    - *For small deals (startups with 10 to 20 people) it is usually up to 3 months*
    - *For big deals (medium and large companies in excess of 500 people), up to 2 years to complete. In the first year, 80% work is done. In the second year there is about 20% remaining like aligning sales teams etc.*
16. In your experience how was access control managed in most deals where you were not responsible for setting these up?

- *In most deals, it was not managed upfront. Instead when I came onboard I tried to put together access control management.*

17. What are your suggestions regarding onboarding acquisitions?
    - *Security must be addressed right up front.*
    - *Communication is important with respect to access to information as files are put in the repository during the entire onboarding lifecycle.*

5.2.5 Interview with an Industry Expert in M&A

1. What is your name? – left out for confidentiality
2. Where do you work? – company name left out for confidentiality
   I am a senior VP of a company that facilitates mergers and acquisitions.
3. How much experience do you have in M&A?
   More than 15 years in managing acquisitions onboarding at multiple companies. I have experience in acquisitions of small companies and big companies.
4. What is your role in acquisition process?
   - *Leading the corporate strategy process and developing the M&A strategy.*
   - *Leading due diligence teams, facilitating the internal and external processes*
     - *Internal processes*

       Getting buy-in from executives, operations management of the process, building the business case for acquisition, presentations for exec team and the board.

     - *External processes*

       Work with the acquired company, interface with the necessary financial and legal teams outside of the company etc.
   - *Three key work streams initiated in due diligence:*

1) *Commercial – looking at operations, integration issues, and synergies between the two companies. Assign work stream leaders.*
2) *Legal*
3) *Financial*

- *In onboarding, Five to Fifteen work streams in HR, IT, Sales and Marketing, Product Management, Engineering etc. are initiated.*

5. Do you consider access control mechanisms in onboarding collaboration?
   - *Yes*
6. Please explain how you handled access control management
   - *Access control was set up beginning with due diligence.*
   - *Folders were created for multiple work streams and for each folder access control was defined. Access to these folders was set up by function.*
   - *Each functional team also assigned access control to files in their folders*
   - *For information pertaining to confidential employee information like salary very high access control was set up.*
7. What tools did you use to manage access?
   - *Used a variety of tools like Merril, Share Point, Drop Box, Box etc.*
8. How did you manage access to the target company?
   - *Communication was established with the functional teams between the two companies*
   - *These functional teams collaborated using the collaboration tools.*
9. At what level did you specify access control?
   - *Roles and responsibilities influenced access control*
   - *The entire deal team list was maintained. It included all participants involved in the acquisition. They all had to sign an internal NDA.*
   - *The access control was then set up at folder and file level. Use email id was used as an access control mechanism.*

10. How would you know if someone leaves a target/acquired company or the acquiring company?
    - *Internally, there are multiple touch points that will ensure propagation of this information.*
    - *The acquired company has to maintain their own processes to manage this.*
11. When someone requests access via email what actions do you take?
    - *If it is at my level of responsibility I look at their role and responsibility and take the necessary action*
    - *I also delegate the decision to the corresponding functional team*
12. Is the acquisition onboarding process well-defined?
    - *Big companies where I was involved usually have some process that is defined satisfactorily but that could be improved.*
    - *The small to medium size companies do not have this process well-defined.*
13. When does integration start in your expert opinion?
    - *Integration starts before the deal closes.*
    - *The term sheet is a good starting point to consider as integration starting point because it has an integration plan in theory*
    - *Integration plan is signed off as part of deal closure.*
14. What teams were involved in acquisition onboarding in your experience?
    - *HR, IT, Product Management, Engineering, Finance, Legal, Sales, etc.*
15. What is the length of time for completing acquisitions onboarding?
    - *For small deals (startups with 10 to 20 people) it is usually one to three months*
    - *For big deals (medium and large companies in excess of 500 people), it is from six to eighteen months. The back office integration (all processes except product integration) is usually done in about nine months. The product integration is anywhere from six to eighteen months.*

16. In your experience how was security managed in most deals where you were not responsible for setting these up?
    - *Access control was managed by the deal leads and was controlled at the functional level.*
    - *Trust management was essentially at the level of functional lead.*
17. What are your suggestions regarding onboarding acquisitions?
    - *Security is a people issue and one has to trust people.*
    - *Insider list which contains all people involved in onboarding should be maintained. They have to sign NDAs when they come onboard.*
    - *Access control should be established based on roles and responsibilities and determined at the functional level.*
    - *Dynamic access control decisions should be at the functional level*
    - *An onboarding collaboration process should be defined to manage security.*

The next section presents a discussion on pilot survey administration and insights.

5.3 Pilot Survey Administration

The pilot survey was administered to a small group of four people (two of them played the role of team leader, two of them played the role of team leader/integration manager; and two of these are also industry experts who facilitate mergers and acquisitions). It was also used as a means of interviewing two industry experts to ensure that the survey objectives, type of questions and the content are appropriate for collecting the data suited for this research. In addition, it also provided insights into the access control management challenges that require further research and investigation. The pilot questionnaire is shown in Appendix B. The key insights from the survey are as follows:

1. Role and Responsibilities

Only three of them “completely agreed” that their roles and responsibilities were clearly defined, while the other “somewhat agreed”.

2. Collaboration Team

   Two of the participants did not have a clear understanding of their immediate collaboration team members

3. Information Control and Access Control Management

   Only one participant checked “completely agree” that information sharing and access control management in onboarding was explained in the beginning while the other three only checked “somewhat agree”.

4. Method of sharing documents

   A combination of email, drop box, and internal collaboration space are used by all participants.

5. Access Control set up for documents shared

   While two of the participants (one a team leader while the other a team leader and integration manager) specified access control for the documents that they shared, the other two did not.

6. Access to onboarding related documents

   All of them had access to all the documents in the repository

7. Requesting access to documents

   While three of the participants said that they receive emails from other onboarding team members requesting access to their documents, only one participant cited that their internal collaboration system has features that allow other to request access to documents.

8. Granting access to documents

   Two of the participants email documents requested in addition to using collaboration workspace to grant access. The other two participants use collaboration workspace to grant access.

9. Accessing other documents in collaboration workspace

   While only one participant said that they did not open other documents, the reaming three said that they often opened other documents to gain a broader understanding.

10. Clarity of onboarding process

    All the survey participants said that they had complete clarity of the process.

    Beginning and Ending of Role in onboarding

11. Only two thought that they had complete clarity as to when their role begins and ends in onboarding lifecycle while the other thought they only had partial clarity.
12. Inter-enterprise collaboration process is defined completely and accurately

    Only two participants completely agreed, while the other two somewhat agreed.

13. Risk Management Strategies to manage project timelines and personnel changes

    While two participants completely agreed that these were well-defined, the other two only agreed partially.

14. Access to onboarding documents when a person's role terminated

    All participants said that when a person's role was terminated, they still had access to documents in the repository sometimes even after the onboarding project was complete.

15. Onboarding project closure

    Only one participant complete agreed that project closure was defined clearly. One participant somewhat disagreed that it was defined clearly. The other two only agreed partially that project closure was defined clearly.

16. Assignment of roles and access control

    Only two participants thought that assignment of roles and access control is defined clearly while the other two only agreed partially with this statement.

17. Trust management in access control

    Two participants said they use trust management schemes dynamically to grant access, one participant said that they only use statically defined access control, while the other participant said that they email documents when they trust a person.

18. Notifications

Only one participant said that the system notifies everyone when a document is added. The other participants said that sometimes they receive emails from individuals who put documents in the repository.

19. State your opinion on how effectively collaboration security in terms of access control is managed in onboarding

    One participant said that this question is phrased in a confusing manner. One opined that it is essentially not done effectively. The other two participants said that measures such as signing non-disclosures, setting up clear security mechanisms, new team members endorsed by team leader, and some central control are required to have effective collaboration security in onboarding.

These results show that the areas of improvement in managing access control in dynamic collaboration in onboarding encompass process, statically defined security mechanisms, dynamic access control schemes based on trust, procedures such as NDAs, and a proper set of activities from beginning to the closure of the onboarding lifecycle. This research is focused on development of a process and access control model to address these issues. Based on this preliminary survey and the feedback that the respondents provided about the clarity of questions, the questionnaire was modified and administered to 25 participants. The results of the survey from this list of participants and the insights are presented in the next section.

5.4 Updated Survey Administration

The pilot survey questionnaire administration has resulted in modifying the questionnaire accordingly to ensure that questions are clear without any ambiguity, and the choices more appropriate. For example a question on risk management in the questionnaire used for pilot is:

Risk Management strategies were well defined to manage project timelines and personnel changes

Mark only one oval.

- ○ completely agree
- ○ somewhat agree
- ○ somewhat disagree
- ○ completely disagree

This question turned out to be ambiguous from the respondents' answers. On reflection, it was understood that in the case of project timelines the respondents may answer one way but in the case of personnel changes it could be different. In the final survey questionnaire, the above question was split into two questions, one for project timelines, and the other for personnel changes. Another example that illustrates the types of wording changes is the choices given for answers to a question. For example a question from the pilot survey questionnaire was:

My roles and responsibilities are clearly defined in on boarding *

Mark only one oval.

- ○ completely agree
- ○ somewhat agree
- ○ somewhat disagree
- ○ completely disagree

This was changed to the following in the updated survey questionnaire as:

My roles and responsibilities are clearly defined in onboarding *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

The phrase *completely agree* in pilot questionnaire suggested that a participant agrees 100%. This is changed in the updated questionnaire to *strongly agree* which resonated better with participants. The updated survey was administered to 25 participants in the industry. Appendix C shows the survey form.

The results of the survey are shown in Appendix D. It shows the summary analysis of each of the survey questions. It also includes their comments in the open questions. It should be noted that the summary questions where the participants expressed their thought and opinions shows a few grammatical and spelling errors which are left as is to maintain the integrity of the survey. Additional details of the survey are as follows:

1. Company Profiles

   The participants worked in large companies including high tech, health care and pharmaceutical industries, retail, IT services, and ecommerce. In addition participants also came from medium sized companies in high tech, IT services, and training organizations. Finally, the survey participants included industry experts who facilitated mergers and acquisitions through their consulting organizations.

2. Survey Participants background

   The participants on average have more than 15+ years of experience in the industry. The survey participants list includes CTOs, senior managers and executives of Engineering, Marketing, Sales, and IT, technical and business

leads, learning and development executives, specialists in mergers and acquisitions, and project managers.

3. Follow Up

   The survey further enabled identifying a short list of participants who will be approached for model validation.

The next section presents a further analysis and interpretation of the survey results which will influence the development of the model.

5.5 Analysis and Interpretation

Research investigation typically includes primary data collection and analysis phase. This step provides a researcher with additional insights that complement the data gathered through secondary research data collection like literature review. The survey conducted provided insights that enable the development of a model to address the security issues in onboarding collaboration. This section provides an analysis and interpretation of results and discusses the insights that will influence the development of the access control model.

The results are analyzed and interpreted under the following categories: 1) roles and responsibilities, 2) access control, 3) risk management, 4) trust management, 5) onboarding collaboration process, and 6) opinions.

1. **Role and Responsibilities**

   - 30% of the participants thought that their roles and responsibilities were not clearly defined. However, the team leaders thought that their roles and responsibilities were clearly defined. 24% of the participants thought that they did not have a clear understanding of the roles and responsibilities of their collaboration team members.

- 20% of the participants did not have a clear idea about when their role begins and ends, while 56% had partial idea about when their role begins and ends.

The issue here is that when people were brought into teams during the course of onboarding their given roles and responsibilities were not defined comprehensively and their relationship with respect to rest of the team members lacked clarity and understanding. Also, from the view point of security, if there is no clarity about when a role begins and ends, it will lead to vulnerabilities which in turn may pose information leakage risks.

2. Access Control

- Only 20% agreed that information sharing and access control management was explained to them clearly, while 48% partially agree. 32% percent disagreed that information sharing and access control was defined clearly.
- Only about 33% used internal collaboration space for sharing documents but almost all used mechanisms such as email, Google drive etc. to share documents.
- While the participants said that they specify access control to the documents that they shared (either they set it up or work with the team leader), 56% of them also said that they had access to all documents in the repository during onboarding
- 21 % of participants said that they email documents to people when they request access while the others use the internal collaboration space and approval of team leaders to grant access

The issue here is that access control is something that is not consistent across different teams and different organizations. While there was some form of access control, there was lack of well-defined process and sustained effort to enforce access control during onboarding collaboration.

3. **Risk Management**

- 75% of the respondents said that they accessed other documents in the repository either to find out if they needed the document or to gain a broader understanding.
- Almost 33% participants said that risk management strategies were not well-defined.
- 68% of participants had access to documents in the collaboration repository even after their participation ended.
- The issue here is that inadequate measures were put in place for risk management in controlling who had access to information assets, and not having defined procedures to manage access.

4. **Trust Management**

- 20% of the participants shared documents based on their individual trust while another 20% said that they used trust management techniques to grant access dynamically during the onboarding lifecycle. 44% said that all access control is determined through statically defined policies.

The issue here is that most of the access was determined through statically defined policies upfront while sharing in dynamic collaboration was not yet a well-defined process because these were shared based on individual trust outside of the collaboration space.

5. **Onboarding Collaboration Process**

- 32% thought that the process is poorly defined while a further 64% partially agreed that the process is well-defined.
- About 33% thought that process milestones, metrics for measuring project progress, and project closure were inadequately defined. About 60% partially agreed that these are defined adequately.

- Almost 75% respondents only had partial idea about when their role begins and ends during the onboarding process.

The issue here is that one of poor process which in turn led to inadequate security. The fact that people did not have a clear understanding of their roles, responsibilities, when their role begins and ends, and what access control management is in place, there was potential for security lapses with negative consequences.

6. Opinions

- Almost all opinions of the participants suggest that onboarding collaboration process, access control mechanisms, dynamic trust management must be addressed (the complete list of opinions are in Appendix D).

5.6 Insights and Observations

The previous section has given insights in the context of analysis and interpretation of results. The survey reinforced that access control in onboarding is an area that needs to be researched further. At the outset, two critical issues are identified: 1) onboarding collaboration process, and 2) access control in dynamic collaboration. In the onboarding process, people should have a clear understanding of their roles and relationships with their collaboration team members, and they should have clearly defined access to collaboration repository. A good process on onboarding collaboration provides a foundation for managing access to collaboration space. The key access control objective in the context of onboarding is one of confidentiality and integrity. Enforcing confidentiality prevents leakage of business sensitive information. The survey clearly

showed that there is leakage of information when access control is poorly designed. In this context the data analysis showed that the individuals use their personal trust to share access to their documents. Instead trust should be managed dynamically in onboarding based on certain criteria defined by the collaboration team. The factors that the model will consider from the survey are as follows:

- Security requirements must be stated upfront
- Collaboration onboarding process lifecycle must be defined
- Security in managing onboarding must be addressed
- Formation of integration teams in the lifecycle must be considered
- Enterprise Roles in access control must be defined
- Governance and static access control policies must be defined upfront
- Change management must be addressed

5.7 Summary

This chapter has presented the details of the data collection and analysis. The case study, pilot survey, and the final survey provided insights into the research issues that need to be addressed. Tow specific aspects of onboarding collaboration are the collaboration process and access control. The next chapter presents an access control model in onboarding which also addresses trust management in dynamic collaboration.

6 Access Control in Onboarding

"Simplicity is the ultimate sophistication" -- Leonardo da Vinci

6.1 Introduction

The industry experience, research review, data collection through survey administration, interviews, and the subsequent critical analysis reinforced the need for addressing access control in onboarding where inter-enterprise collaboration is the means through which the integration and assimilation of acquired company is completed. In today's competitive business world, information leakages whether malicious or accidental could potentially harm companies and organizations. The negative consequences could include anything from financial losses, losing competitive advantage, legal lawsuits, brand getting tarnished and even insolvency. In essence protecting information assets should not be an afterthought; it must be integral to the conduct of a business. In the opinion implied by this research and reinforced by industry experts, information protection is a way of life in the conduct of a business. This approach implies that when a company acquires another company, it must integrate all aspects of security including access control during the lifecycle of onboarding until the acquired company is integrated and assimilated into the company and the project is officially closed.

The literature review revealed that 1) access control management in inter-enterprise collaboration in the context of onboarding is not directly addressed, 2) role-based access control continues to evolve to address new collaboration processes, and 3) trust plays a role in access control management in dynamic environment. The data

collection, analysis, and survey results revealed that 1) access control in onboarding is an area that needs to be researched further, 2) there must be well-defined onboarding collaboration process model, 3) there must be clearly defined roles and responsibilities in dynamic collaboration, and 4) security must be addressed throughout onboarding collaboration. These insights lead to the development of an onboarding collaboration process model and further lead to integrating security across the process model.

This chapter presents an access control model based on this research undertaking. First, it begins with a discussion of the foundational element on which the model rests: *onboarding collaboration process*. The process provides a reference to discuss security aspects of collaboration. Next, a discussion on the concepts of enterprise roles and collaboration roles is presented. Every person involved in the collaboration has these two roles because of their association with their own company to which they belong to and because of the fact that they collaborate during the onboarding process. The notion of trust is introduced and concepts such as weak trust and strong trust are discussed. These concepts influence the dynamic access control decisions influenced by trust. The notion of *security touch points* is introduced to essentially show the interfaces and points in the process lifecycle of onboarding where information security must be addressed in order to prevent either accidental or malicious leakage of information. In the context of security touch points, the idea of security requirements is presented as well. The concept of self-organizing systems is discussed to show how in this model, the access control distributed knowledge base evolves as new information and knowledge is gained in the onboarding lifecycle. During the process of collaboration,

information assets are added, updated, or deleted. A discussion on change management is included to show the ramifications of administering the proposed access control management solution. The section on change management includes a discussion on publish/subscribe mechanism for secure collaboration. An illustrative example scenario of onboarding is discussed to showcase the inner-working of this access control model.

6.2 Secure CODA (Create, Operate, Dissolve, Archive) Onboarding Collaboration Process Model -- SCODA

The chapter on onboarding (Chapter 2) presented representative works in the literature on onboarding processes in the context of mergers and acquisitions such as those discussed in [2] and [20]. While they describe the process from the view point of a strategy for business growth, this research focuses on specific aspects of onboarding a company that has been in principle acquired. This is the starting point for this process. This starting point is characterized by certain attributes which will be discussed in detail in this section. Likewise, while the M&A literature describes the legal closure of acquisition process, this research narrowly focuses on closure with its own set of characteristics that signify closure. Between the starting point and the closure, there are processes related to creation and operation of necessary collaboration teams to onboard people, processes, technologies etc. This section provides reference process steps for discussing collaboration security. In addition to closure, this research proposes and defines the concept of archiving to ensure that once onboarding comes to a closure all the information assets shared by collaboration is systematically archived from the perspective of collaboration security.

Collaboration signifies a team of at least two entities. The definition of an entity from the perspective of this research is as follows:

Definition: Entity

> *The entity could be a person, process, business unit or department, or an organization as a whole.*

In the context of the global process of M&As where acquisitions are part of an overall business strategy, different internal teams are formed within an organization to perform various tasks aligned with business strategy. This part of the global process is not of concern to this research. Instead, the process discussed in this research is only in the context of teams formed comprising of people from both the acquiring and acquired companies. This is often characterized by the formation an *Acquisition team*. Figure 6.1 shows the starting point of this process. The chapter on onboarding describes this global process in more detail. In all approaches at some point in the overall acquisition lifecycle an acquisition team is formed and this is the reference point for this research. The steps shown in Figure 6.1 are based on the discussion in [2].

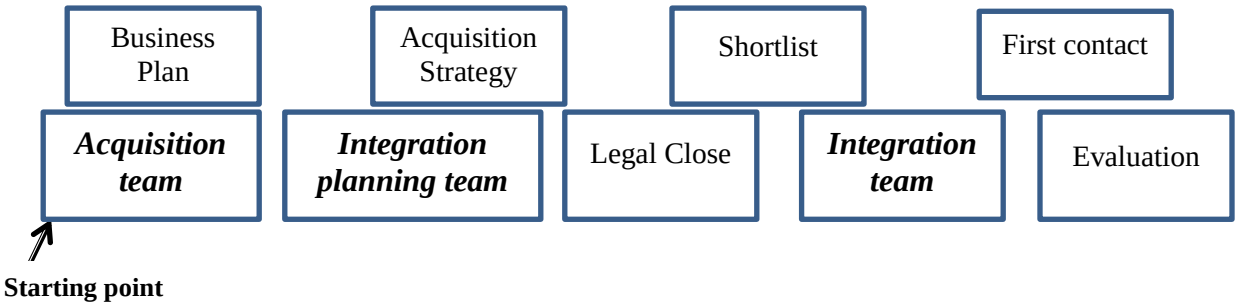


Figure 6-1: Starting point for inter-enterprise collaboration in onboarding

It depicts three inter-enterprise collaboration teams at the highest level: 1) Acquisition team, 2) Integration Planning team, and 3) Integration team. These three teams further

drive the rest of the process activities in onboarding the acquired company. This research proposes a secure onboarding collaboration process model, called SCODA, for onboarding collaboration activities among the inter-enterprise teams. The model emphasizes a four phase collaboration lifecycle that begins with a *creation phase* where collaborating teams are created. Security is built-in in all phases of the model (hence the name SCODA). These inter-enterprise teams work together on a collection of activities in the context of onboarding. This working together is characterized by the *operations phase*. Once the task of onboarding is accomplished, the team is dissolved characterized by the *dissolve phase.* The information assets of the project are then archived in the *archive phase*. Figure 6.2 shows the SCODA model and puts it in perspective with the collaboration teams formed during the onboarding lifecycle.

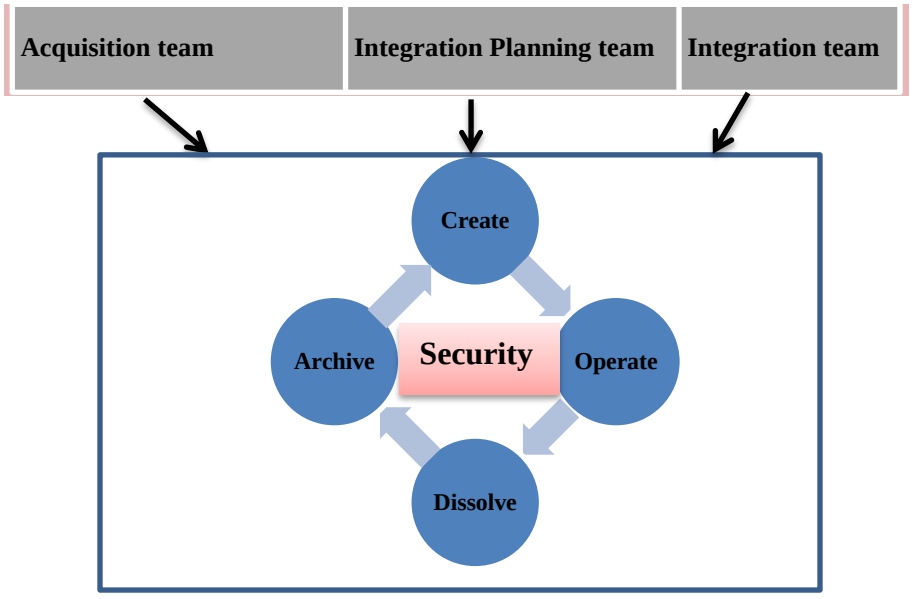


Figure 6-2: SCODA process model

Every team that is formed during the onboarding should adhere to the SCODA process model to streamline security and access control so that information assets are protected

during and after onboarding is complete. Security is something that should be built into the process lifecycle right from the beginning of the process until it ends, just as how quality must be built-in to any process. This model implies that it can be integrated seamlessly into any well-defined onboarding process model that companies may have because this model overlays during their process at points where collaboration teams are formed during the onboarding lifecycle. The model also suggests that the three key collaboration team forming stages as shown in Figure 6.1 are where access control should be addressed.

6.2.1.1 Create

This phase triggers the beginning of the inter-enterprise collaboration of the respective teams in the onboarding lifecycle. While some teams may exist from the beginning of the onboarding process, other teams may be formed during the specific time intervals in the overall project scope. Irrespective of when a team comes into existence, every team must perform a certain set of collaboration starting activities which this research defines as *Baseline Collaboration Tasks*.

Definition: Baseline Collaboration Tasks

> *A collection of tasks performed by the collaboration team when it first comes into existence.*

The set of tasks performed at creation may vary by the team and their charter. However, the set of baseline tasks that every team must perform, when they come into existence, include the following: 1) identify enterprise roles, 2) define collaboration roles,

3) identify the baseline information content in the collaboration work space, and 4) identify security requirements from the viewpoint of access control to information assets.

The enterprise role and the collaboration role enable the identification of the responsibilities of the team members. An enterprise role further allows insights into the access privileges to information. The collaboration role access privileges are baselined in the creation phase as a community activity where the team determines what those privileges are. The details of the concepts of enterprise role and collaboration are discussed in the following section. It is also in this phase that the team sets a baseline of security requirements in terms of who has access to information repository. This is an iterative community driven process between the collaboration roles, access privileges and security requirements.

6.2.1.2 Operate

This phase is characterized by a collection of tasks performed by the respective collaboration team members. This phase could be called an active phase of onboarding lifecycle where participants are constantly interacting, requesting and sharing documents, requesting access to applications, processes etc. It is also characterized by the fact that the team composition itself may be subject to change. Access control becomes a critical issue. The security requirements defined in the Create phase provide a foundation for determining access. However, in the active working environment in this phase, access decisions are governed by statically defined policies and also the dynamic access policies as characterized by *trust relationships*. The concepts of trust and trust relationships are defined in the following sections. Later in the chapter, a

simulated example will demonstrate how these concepts come together to manage access control in inter-enterprise collaboration.

6.2.1.3 Dissolve

This phase is characterized by the completion of tasks associated with a collaboration team. From a security and access control management viewpoint, a systematic collection of tasks need to be performed in order to ensure that information assets are protected and are not available to the collaboration team members beyond a specified time. Key tasks in this phase include: 1) signing off the completion, 2) reviewing access privileges to assess who further requires access to information assets for some length of time, 3) taking end-of-life decisions to terminate/restrict access of roles and people and 4) reviewing the roles, responsibilities, and security requirements with reference to baseline and documenting the necessary continuous process improvements. For example, the dynamic collaboration may have shown that some additional information assets must have been put in the repository at the beginning; collaboration roles may have been updated with additional tasks, some additional access rights may have been added, some access rights may have been found to be either redundant or not required etc.

6.2.1.4 Archive

This is a step that is critical to business security. The survey results indicated that most people had access to the information assets well beyond the closure of the acquisition onboarding. This could potentially lead to either accidental or malicious leakage of business sensitive information. In the SCODA model, this phase of the collaboration

lifecycle is mandatory. The key tasks in this phase include: 1) archiving the information assets based on the overall enterprise security framework and data management, 2) having a designated process to restore archived data in the future for any purpose including denoting the enterprise role that is required to request retrieval of archived data.

6.3 Roles in Onboarding Collaboration

Role based access control is a well-known paradigm as discussed in the literature review of this research. In 1992, Ferraiolo and Kuhn [147] , integrated the then features of existing application-specific approaches such as the discretionary access control and mandatory access control policies into a generalized role-based access control (RBAC) model. The model went through subsequent iterations and in 2001 a reference model for role based access control was proposed [148]. RBAC model addressed the security management challenges associated with Discretionary and Mandatory access control models. Discretionary Access Control (DAC) is very flexible and allows incorrect and wrong behaviors in organizations that are poorly managed, while Mandatory Access Control (MAC) is suited for organizations connected with high security or for government organizations such as US Department of Defense where multiple levels of security clearances are required. There was a need to support subject-based security policies, such as access based on competency, conflict of interest rules, or access based on a strict concept of least privilege. At the same time it was important to work within the context where there is a hierarchy of roles. RBAC model fulfilled these needs. A key feature of this model is that all access is through roles. A role is essentially a

collection of permissions, and all users receive permissions only through the roles to which they are assigned. Figure 6.3 depicts a simple conceptual model of RBAC. Users are assigned to roles and roles have permissions. Permission is an approval to perform an operation on one or more RBAC protected objects. For example, if the object is a file, operations on the file include read, write, and update. If an object is a database table, the operations on the table could be insert, delete, and update.

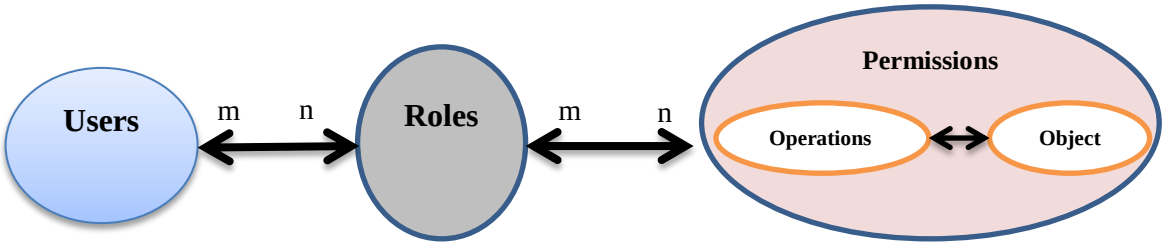


Figure 6-3: A simple conceptual model of RBAC

The RBAC model continued to evolve with numerous variations and extensions to address issues like the administrative overheads of role management [149], granularity of permissions at attribute level [150], different hierarchical relations between roles [151] etc. The change management issues associated with RBAC model from a security management perspective is discussed by this researcher in [7] wherein it is proposed that a clear distinction be made between an *enterprise role and functional role.* This distinction allows for smaller set of enterprise roles which further simplifies RBAC model based security management.

From the perspective of this research, three types of roles are important for access control in inter-enterprise collaboration: 1) Enterprise Role, 2) Functional Role and 3) Collaboration Role. The person participating in collaboration belongs to an organization

where they have assigned enterprise and functional roles in different groups within the enterprise. For example, one person could be classified in an enterprise role as *Manager* and have a functional role *IT Manager* in the function group IT operations, while another person could be assigned an enterprise role *Engineering* and he/she may be performing a functional role of *product engineer* in a functional group producing tablet PCs. In addition to these roles a person plays specific roles in inter-enterprise collaboration. For example, a person could be team leader in collaboration while also playing the role of IT architect. In the context of this research the concept of a resource is also relevant. This concept is similar to the concept of objects (shown in Figure 6.3) but more specifically defined in the context of this research. The definitions and examples of resource, an enterprise role, functional role and collaboration role are discussed next.

6.3.1 Resource

The concept of a resource is a foundation element in the SCODA model developed in this research. The model relies on the concepts of *users, roles, and* resources. Figure 4 depicts the relationships between users, roles, and resources. Resources exemplify the processes, applications and data that users have access to when performing their roles. Users may be assigned to one or more roles. A user will have access to a range of applications and data as part of fulfilling a role. In other words, access control is established in the context of roles. For example, user “John”, assigned to the role “sales manager”, will have access to sales applications and associated data. The same user assigned to the role “marketing manager” will additionally have access to marketing applications and associated data. If John were assigned the role “sales manager —

Asia" he would only have access to the sales applications and data relating to Asia. The formal definition of a resource is as follows:

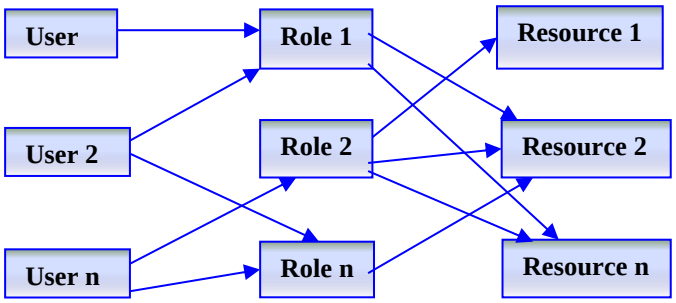


Figure 6-4: Adapted RBAC (see Figure 6.3): Users, Roles, and Resources

Definition: Resource

A resource is a tuple Res (ObjName, DataSet), where ObjName is the resource name and DataSet is the collection of atomic data (metadata).

Example: a resource could be "customer tracking system" (CTS), comprising of customer name, address and status. It is expressed as:

Res (CTS, {customer name, customer address, customer status…}).

The definition of resource is used in the subsequent definition of various roles. It should be noted that the roles are mapped to resources in this role based access control model unlike in the RBAC model shown in Figure 6.3. The permissions as to what operations can be performed on objects by a given role are best denoted as attributes of the access relationship between a role and a resource. Furthermore, the notion of a resource provides a higher level of abstraction in terms of the semantics as it denotes classes of information unlike an individual object. Such a representation provides an

advantage in terms of understanding access control at a higher level of abstraction before delving into fine-grain access control at individual object level.

6.3.2 Enterprise Role

The definition of an enterprise role is in the context of a business. In large organizations, the human resources function typically defines enterprise-wide roles. These are job categories, such as “CEO”, “VP”, “Engineering”, “Sales”, etc., typically characterized by the collection of responsibilities and tasks that are performed by the individual who is assigned the role. A distinguishing characteristic of such a role is that it is general in scope and allows an organization to abstract and categorize cohesive sets of job responsibilities.

Definition: Enterprise Role

> *An enterprise role is a tuple ERole (ERName, Rlist), where ERName is the enterprise role name and Rlist is a named collection of tasks/responsibilities.*
>
> **Example:** an enterprise role “customer relationship manager” can be defined as:
>
> ERole (customer relationship manager, {customer needs analysis, track Projects…}).
>
> In this example, the role “customer relationship manager” is the ERName, and the role list (Rlist) comprises tasks performed by users assigned to that role.

In this definition of enterprise role there is no specification of the actual resource/data access control rules. Enterprise roles should capture only the essence of job functions without any consideration of resource/data visibility rules.

6.3.3 Functional Role

Like the enterprise role, a functional role is in the context of a business. It can be viewed in terms of day-to-day functions that an individual performs within a functional unit in an organization. For example, at enterprise level an individual may have a role such as “engineer”. Within a specific department, the individual’s role may be “analyst”, “program manager” etc. The greater specificity implies not only the specific tasks that the individual performs but also the specific information, applications, processes to which the individual has access to. Detailed access control is pertinent in a functional role where the tasks are defined at a finer granularity that entails accessing specific resources with privileges such as read, write, update, execute, etc. The definition of a functional role is as follows:

Definition: Functional Role

A functional role is a tuple FRole (FRname, ERName, Res, PrivSet), where FRname is the functional role name, ERName is the enterprise role name, Res is the resource and PrivSet is the set of privileges accorded to this role on the data set associated with the resource.

Example: Consider a customer tracking system (CTS). Here, a functional role associated with this system could be:

FRole (site manager, customer relationship manager, CTS, {(customer name, R), (customer address, U), (customer status, R)}).

In this example, a functional role *site manager* is defined, and users assigned to this role can only read (R) customer name and customer status and update (U) customer address. It further specifies that this role is associated with the enterprise role *customer relationship manager*.

6.3.4 Collaboration Role

Onboarding collaboration is a process with an outcome. Teams are created which include members from both the acquiring and acquired company. There is starting point of this collaboration and an ending point as characterized in SCODA model discussed in this chapter. During the course of collaboration roles and responsibilities are assigned to members of the collaborative team in the creation phase. These roles are called *collaboration roles*. The properties of these collaboration roles are:

- Collaboration roles are transient. These roles exist in the context of collaboration. Once the onboarding is complete, these roles are deactivated.
- Collaboration roles are weak or secondary roles and can only exist along with the corresponding primary enterprise roles in the context of onboarding.

The property of a weak role is akin to the concept of a weak entity in Entity-Relationship modeling [152]. It exists only in the context of the primary enterprise role and it is a transient role which gets deactivated once onboarding collaboration ends. Later in the chapter, the consequence of having an associated enterprise role is further examined in making dynamic trust based access control decisions. The definition of a collaboration role is as follows:

Definition: Collaboration Role

A collaboration role is a tuple CRole (CRname, {ERName,Org_name}, Res, PrivSet), where CRname is the collaboration role name, {ERName,Org_name} provides the enterprise role name associated with the respective organization, Res is the resource added to the collaboration workspace and PrivSet is the set of privileges accorded to this role on the data set associated with the resource.

Example: Consider an inter-enterprise IT collaboration team formed to integrate customer databases of two companies ABC, and XYZ. Here, a collaboration role associated with this system could be:
CRole (Team_Lead, {IT Lead, ABC }, CIS, unrestricted).

In this example, a collaboration role *Team_lead* is defined, and user assigned to this role is an IT Lead with ABC organization with unrestricted access to the resource CIS (Customer Information System).

The SCODA model, the adapted RBAC model emphasizing access control privileges as attributes of relationship between a role and resource, and the definitions of resource, enterprise role, functional role, and collaboration role will pave the way for rest of the discussion in this chapter.

6.4 Security across CODA

In Section 6.2, in the context of discussing the SCODA model (Figure 6.2), it is stated that security must be built into the entire onboarding lifecycle. In this section, this aspect of the process model will be elaborated. First, a discussion on security requirements provides insight into what security means in the general context of undertaking any type

of project – product development, application development etc. This is followed by a discussion on collaborative sharing patterns and access control requirements in dynamic collaboration. Finally, this section discusses how to *build security in* across the onboarding collaboration life cycle.

6.4.1 Security Requirements

There is no general consensus about the definition of *security requirement* in the literature. The term *security* itself is an overloaded term because it means many different things to academic researchers, practitioners, businesses, end users, and government. In today's uncertain world, characterized by terrorism, the word *security* is tagged to everything from national security, energy security, food security, economic security, financial security, etc. These terms have become particularly prevalent in this society after the unfortunate disruptions caused by hackers, international information espionage, terrorists, and the alleged government sponsored network breaches. The nuances of security are presented here because they bring out some fundamental characteristics of what security implies to people, organizations, governments, and the global world we live in. Figure 6.5 lists the essential characteristics embodied in the various forms in which security is discussed.

Loss of Lives	Disruption	Harm
Financial Loss	Liability	Privacy Compromise
Denial of service	Shutdown of systems	Unwarranted disclosure

Figure 6-5: Common characteristics of security

Underlying these characteristics is a sense of losing something that was not intended. In order to prevent such losses, security requirements must be captured right at the beginning of any undertaking so that they can be designed, developed, and monitored across the entire project lifecycle, be it in product or application development, or in undertakings such as onboarding acquisitions. In [153], the author observes that security is a poorly addressed topic in product development and suggests that it should be addressed in the context of functional requirements. Firesmith [154] argues that most engineers and developers are inadequately trained to elicit, analyze, and specify security requirements. Haley [155] observes that standards like US National Institute of Standards and Technology computer security handbook recommend that security requirements be documented in terms of security mechanisms which are essentially treated as functional requirements. The author also argues that defining security requirements as functional requirements leaves out other critical information: what objects need protecting and why the objects need protecting. The author makes a case for treating security requirements as constraints on functional requirements rather than being functional requirements themselves. Tondel et. al [153] present additional insights into various approaches suggested in the literature to capture security requirements based on use cases, misuse/abuse cases, security goals, information assets, process planning etc.

For this research the definition of security requirement begins with the question:

What does security mean to an organization?

This is the approach discussed by the well-known security researcher Matt Bishop in his paper [156]. It is self-evident that security has the nuances depicted in Figure 6.5, but

what this question implies is that organizations may have certain requirements that should be met. For example, consider an educational institution that provides courses online and also access to a student information system that includes grade and other student pertinent information. They probably require that this system be accessible online via the internet to students and faculty. They may also require that confidentiality and integrity of grades and other data, which is student specific, be maintained. For them this is a security requirement. Contrast this to a highly secretive government organization like an intelligence department. This department may require that confidentiality of all data is maintained and they may further require that internet access and telecommuting be prohibited. They may not want their staff working remotely to download confidential data into their home computers which may not meet the security standards of the intelligence department.

These examples illustrate why security requirements are really about what security means to an organization. In order to define a security requirement from the perspective of this research, another attribute is considered, the notion of *Risk*. From a practical perspective, risk provides a way to quantify and take a meaningful decision about whether a requirement is really a requirement or not. In addition it also provides additional insights into the type of security mechanisms that should be put in place to secure the object of interest. ISO 31000 (2009)/ISO Guide 73:2002 define risk as follows:

Definition: Risk (ISO 31000 (2009) /ISO Guide 73:2002)

> *Effect of uncertainty on objectives. Uncertainties include events (which may or may not happen) and uncertainties caused by ambiguity or a lack of information. It also includes both negative and positive impacts on objectives.*

In the context of this research, risk has a negative connotation as is characterized in the information security research. This definition of risk is as follows:

Definition: Risk (ISO/IEC 27005:2008)

The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

The definition of security requirements is as follows:

Definition of Security Requirement

A security requirement characterizes what the organization wants to achieve in terms of protecting its information along with an assigned risk (extended from [156]).

It should be noted that this definition is an extension of the notion of the security requirement as discussed in [156]. When a collaboration team comes together, they discuss the roles and responsibilities along with what information assets are put in the collaboration repository. In this context, when they evaluate the risk levels associated with certain information assets, it will allow them to put the necessary security measures in place.

In this research, when designing secure collaboration systems, security is characterized by four components, three of which are adapted from [156], while the fourth component is a contribution of this research.

- Requirements (adapted from [156])
  Define security objectives. They answer the question: “what do you expect security to do for you?”

- Risk (contribution of this research))
  Characterizes the loss when security is compromised either in quantifiable or qualitative terms.
- Policy (adapted from [156])
  A logical design to implement the meaning of security. It answers the question: “what steps do you take to reach the goals set by security requirements?”
- Mechanisms (adapted from [156])
  Implement and manage policies. They answer the question: “what tools, procedures, and other ways do you use to ensure that above policies are followed and adhered to?”

This research also adopts the viewpoint that security requirements are not functional requirements. Instead, they occur only in the context of functional requirements and qualify these with constraints pertaining to what security objectives an organization wants to achieve in the context of implementing the functional requirements. In essence security requirements are contextual in nature. Without a context, there is no reference within which meaningful security requirements can be captured.

6.4.2 Collaboration Patterns and Sharing Requirements

Collaboration Patterns

Collaboration occurs in many domains and varies in scale, size, duration, number of people, etc. On one end of the spectrum is the collaboration that happens in the development of open source software characterized by thousands of people participating, sharing documents, code, etc. On the other end of the spectrum is

collaboration teams of two (by definition collaboration requires two entities/people). From another perspective, there is collaboration between educational institutions, government, industry and university partnerships etc. Underlying all these types of collaboration some distinctive patterns emerge both in terms of the nature of collaboration, organization, relationships, and sharing. The purpose of this section is to discuss these collaborative sharing patterns and put this research in perspective. These classifications are based on insights from this research.

Open vs. Closed

- An open collaboration is characterized by the fact that anyone (an organization or an individual) can participate in collaboration with minimal restrictions or criteria to join the collaboration efforts. Examples of open collaboration include open source development, crowd sourcing, government sponsored research activities and numerous community driven efforts to improve lives of people around the world.
- A closed collaboration is characterized by specific collaboration relationships between two or more entities, most often to accomplish specific objectives. For example, companies collaborate for joint product development, countries collaborate to counter terrorism, and educational institutions collaborate to offer joint programs.

Structured vs. Dynamic

- Structured collaborations are characterized by well-defined processes, procedures, access control management etc. where collaboration

relationships are defined and stable over a period of time. An example of this is GRID based collaboration in virtual organizations.

- Dynamic collaborations are characterized by their ad hoc, spontaneous interactions and usage patterns. An example of this is organizations coming together to work on a joint initiative, typically characterized by a fixed short time duration.

Stable vs. Transient

- Stable collaborations typically have a longer duration and characterized by established access and trust relationships over a longer period of time. For example, organizations which have defined access policies for their defined and established roles fall under this category.
- Transient collaborations are characterized by the temporary nature of collaboration, typically short duration, or with no pre-established trust relationships.

Based on the classification of collaboration patterns, the nature of inter-enterprise collaboration in onboarding considered in this research is classified as *closed, dynamic and transient.*

6.4.3 Sharing Requirements

Collaboration by definition implies sharing of information. In dynamic collaboration the participants share artifacts. The nature of collaboration is such that certain requirements must be in place for successful collaboration. During the course of the collaboration, participants are either added to the collaboration team or they are removed and information assets are constantly added, deleted, or updated. The relationships

themselves are continuously changing with new relationships identified, and existing relationships modified. Due to the dynamic nature of this collaboration it is not possible to define all these systematically at the beginning of collaboration. The essential collaboration sharing requirements identified by this research include:

- Each information asset should have a designated owner so that in the course of collaboration the owner can be included in managing access to the assets.
- Information asset owners should have the capability to define collaboration relationships and access control criteria when they publish the asset into the collaboration space.
- A process for publishing and subscribing to information assets in collaborative space should be established. This will allow that participants a systematic way of publishing information assets into collaboration space and also allow them to request access to information assets.
- A process for managing notifications should be established. During collaboration when changes happen like adding and deleting information assets, personnel changes etc. the notification process is followed.

This set of requirements pertain to the scenario of sharing of information assets, creating the awareness about an information asset inclusion or deletion in the collaboration work space, and ability for participants to request access to information assets. The next section presents access control requirements in dynamic collaboration.

6.5 General Access Control Requirement in Dynamic Collaboration

Access control requirements in dynamic collaboration have been investigated by several researchers. One of the early research papers in early 1990s [98] summarized access control requirements in the context of computer supported Cooperative Work (CSCW) as follows:

- Access control models must be easy to use and transparent for end users.
- Access control-produced effects on the rest of the system must be clear and easy to understand.
- Access control models must allow us great expressiveness (taking into account aspects such as roles, execution tasks, access request data, etc.) and these models should enable us to specify complex access policies at different levels of detail.
- Models must be dynamic so as to enable specification, delegation, revocation and management of access policies in runtime (Meta Access Control).

As new paradigms of dynamic collaborations have evolved, access control requirements to support these environments have evolved too. Additional access control requirements have been discussed in [97], where the author discusses the importance of integrating security elements in the initial models used to understand and describe the system functionalities. A summary of access control requirements for collaborative systems as discussed by various researchers is presented in [153]:

- Access control must be applied and enforced at a distributed level.
- Access control models should be generic and enable access rights to be configured to meet the needs of a wide variety of cooperative tasks and enterprise models.
- Access control for collaboration requires greater scalability in terms of the quantity of operations than tradition single user models.

- Access control models must be able to protect information and resources of any type and at varying levels of granularity.
- Access control models must facilitate transparent access for authorized users and strong exclusion of unauthorized users in a flexible manner that does not constrain collaboration.
- Access control models must allow high level specification of access rights, thereby better managing the increased complexity that collaboration introduces.
- Access control models for collaboration must be dynamic, that is, it should be possible to specify and change policies at runtime depending on the environment or collaboration dynamics.
- Performance and resource costs should be kept within acceptable bounds.

This research agrees with these observations about access control requirements in the context of dynamic collaboration. However, from the perspective of this research the most desirable access control requirements are the following, some of which are above requirements that are reinterpreted and/or restated.

- Security goals should be documented and they in turn drive access control decisions.
- Higher level of abstractions to specify access control should be defined since the abstractions at the participant level only may be difficult because of the challenge of documenting all participants in inter-enterprise collaboration.
- Access to resources should be determined dynamically since statically defined access policies may not necessarily apply due to the dynamic nature of adding new information assets and the transient nature of participants.
- Access control requirements must specify what objects need protection, why they need protection, and an associated risk factor.
- Access to an object controlled by community of participants need to be determined.

- Denial of object access for certain roles need to be determined. This pertains to explicit denial of access.
- Escalation path for access control need to be determined.
- Publish/Subscribe mechanism for information assets need to be determined.

The next section discusses how to build security in using the SCODA model for inter-enterprise collaboration. The abstractions of enterprise, functional, and collaboration roles, the collaboration sharing requirements, and the access control requirements discussed thus far are integral to building the appropriate access control framework in onboarding.

6.6 Building Security in CODA

This section builds on the preliminary discussion on SCODA in section 6.2. It shows the process steps that will enable collaboration teams to discuss roles, responsibilities, security objectives, security requirements in the creation phase. It further shows the steps for access control and management in the operational phase, incorporating the security knowledge discovery (of the operations phase) in the dissolve phase, and taking the necessary security and access control decisions in the archive phase.

6.6.1 Security in the Create Phase

The create phase is characterized by a set of *baseline collaboration tasks* as discussed in Section 6.2. Figure 6.6 depicts the activities in this phase. The details of these steps are as follows:

- Form a team

This is the beginning step for inter-enterprise collaboration to onboard the acquired company. The SCODA model shows three higher levels of abstraction for the team: Acquisition team, Integration planning team, and Integration team. Each of these teams has a specific purpose in onboarding.

Acquisition Team – this team is usually formed when the acquiring company and the to-be acquired company sign an agreement (often called the term sheet in the M&A literature). This team is responsible for conducting due diligence before final approval of the acquisition and the legal close.

Integration Planning Team – this team is usually formed once the legal closure happens. This team is responsible for conducting integration analysis of the two company's products, processes, employees, customers, partners etc. They typically define the various project team tracks and also define the processes, methods, and tools that the onboarding teams use for the entire onboarding lifecycle.

Integration Team – this team is responsible for the actual execution of integration plans. Multiple teams come into existence to execute integration of numerous products, processes, etc. While the integration planning team defines the overall team tracks, the tracks themselves are populated with team members, shared information assets etc.

- Identify Roles and Responsibilities
  The collaboration roles and the tasks are established.
- Identify Information assets
  The set of information assets that the collaboration team needs are specified.
- Specify access control requirements
  Define the access control policies pertinent to the collaboration team.
- Conduct Risk Analysis
  Identify risks associated with the information assets. The risk levels could be qualitative such as High, Medium, and Low. Alternatively, it could be based on whatever the risk analysis schemes that were defined at the enterprise level. The

key insight provided by this step will enable identification of assets that the team is willing to publish for dynamic access control in the community.

- Identify information assets for dynamic access management

  These are the information assets that the team is willing to publish for dynamic access control where other community members could gain access to these assets based on community driven trust.

- Publish information assets

  Put the information assets in the collaboration space and publish.

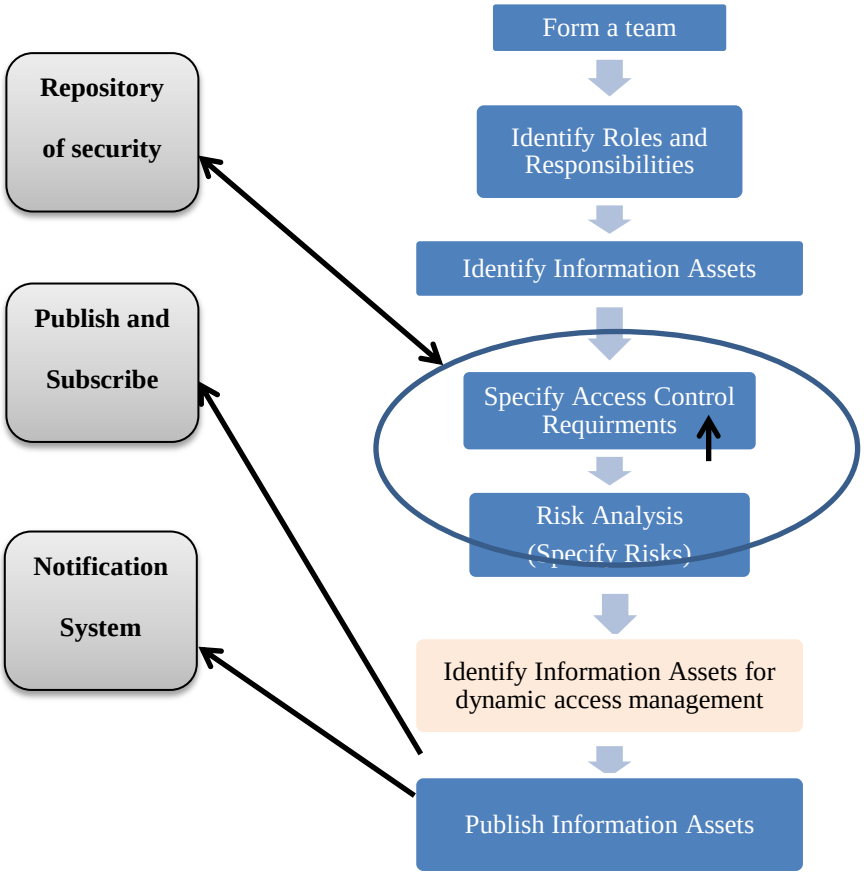


Figure 6-6: Create phase activities

6.6.2 Security in Operate Phase

The operate phase is characterized by the teams undertaking the specific onboarding tasks assigned to the team. For example, assume the team comprises of the sales

personnel from the acquired and the acquiring company. One of the operational tasks for this team is to assimilate the information of the sales business process of the acquired team such as the list of customers, sales pipeline data, etc. In the course of the operate phase new discoveries could be made such as the need to add new information assets into the repository, invite other members to join the team, forming new relationships with other teams, etc. Addressing security must be integral to all these activities in the operate phase. Figure 6.7 depicts the activities in this phase.

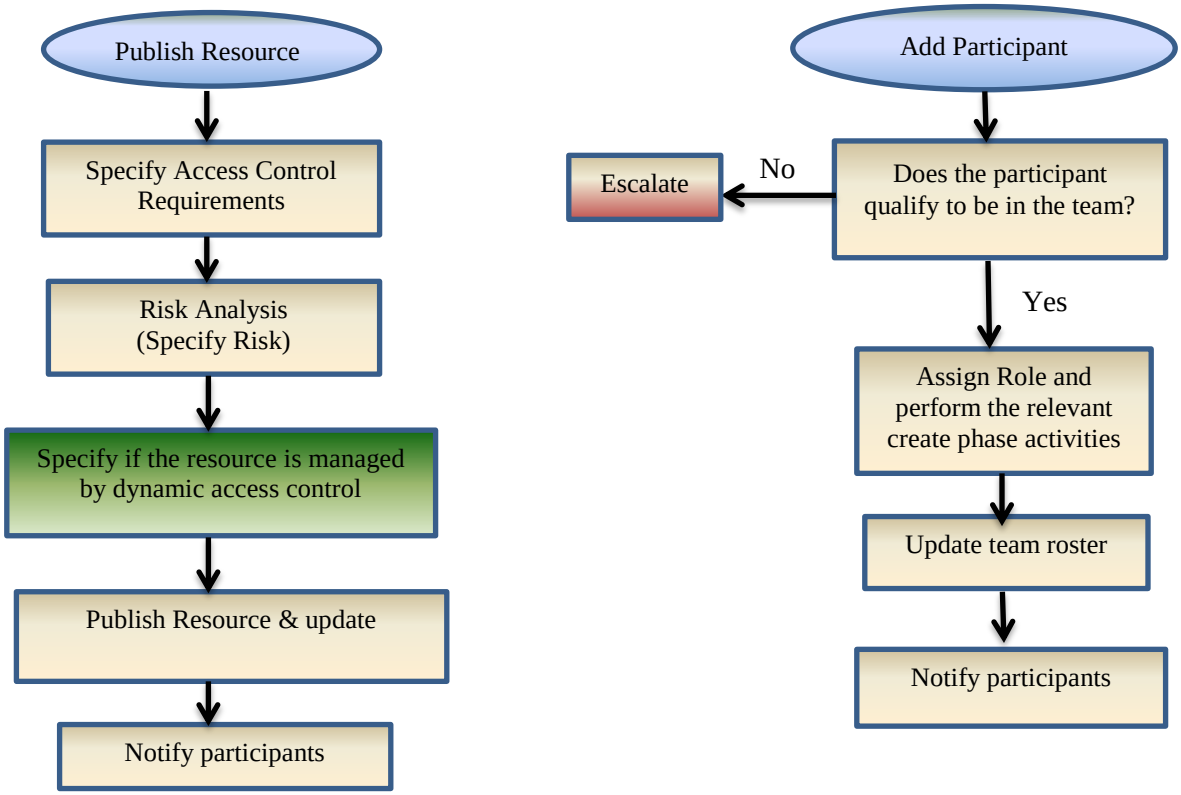


Figure 6-7: Operate phase: publish resource and add participant

Note that for simplicity, the figure does not show the global repository of security objectives, publish and subscribe system, and the notifications systems. They are available as necessary for activities throughout the SCODA lifecycle. In the operate

phase, two other activities are the deletion of a resource from a repository and termination of team members. These should be handled similarly to what has been depicted in Figure 6.7.

6.6.3 Security in Dissolve Phase

This phase essentially signifies terminating the team as soon as their onboarding tasks are completed. Terminating a team is critical from a security viewpoint because termination implies that the team will not have access to business sensitive documents beyond the required time. Figure 6.8 shows these activities.

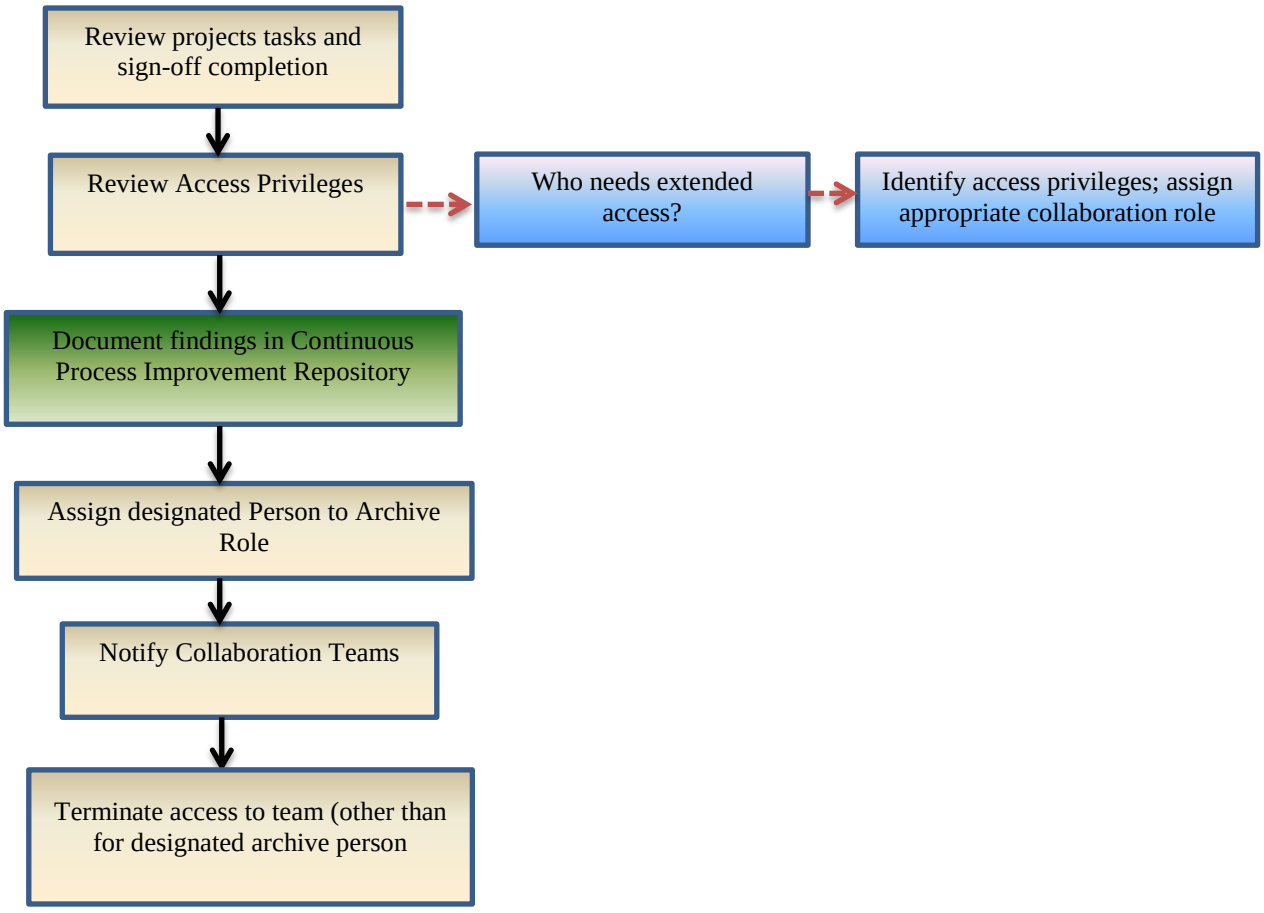


Figure 6-8: Dissolve phase activities

This phase of the SCODA process addresses the concern expressed by survey participants that access to collaboration space has not been terminated promptly after their role ended. In addition, this phase emphasizes the importance of documenting findings of the team in a continuous process improvement repository. The team would have gained knowledge in the course of their collaboration about the collaboration roles and responsibilities, which type of documents were accessed in dynamic collaboration, and which roles may have been added after the team began operations, etc. All this knowledge is useful for future onboarding collaboration endeavors.

The designated archivist in each team is granted extended access at the time of team dissolution. This will facilitate the proper execution of activities in the archive phase where the archivist collaborates with the enterprise IT team.

6.6.4 Security in Archive Phase

The concept of archive is that something is stored away and is not accessible in real time. To gain access to the archived information there will be some processes and procedures to restore and make it available for real time access. In the SCODA model, this is the phase where once the team is dissolved, it is still important to archive the information assets so that they are not available for real time access. The security activities in this phase include identification of a role that has authority to restore archived information assets, determining if a particular information asset need to be archived etc. From the viewpoint of the SCODA model this phase is a recommended step for all collaborating teams. However, the actual archiving authority may rest with one designated team in the overall onboarding process lifecycle. In this case, when a

team dissolves, the authorized archive person has to collaborate with the designated archive team.

This section discussed how to build security across the onboarding collaboration lifecycle. It emphasized how organizations must define what security means to them in onboarding collaboration. This will further drive identification of security requirements. The concept of *risk and risk analysis* is integrated in security requirements. This will provide guidance to the collaboration team to identify those information assets that they could possibly publish and let other teams in collaboration access dynamically without statically defined access policies. The next section discusses how these information assets are accessed dynamically based on the concept of *Trust*.

6.7 Trust in Dynamic Collaboration

Trust is a mechanism studied in the information security literature in making access control decision in dynamic collaboration. It is often not possible to define all access control policies up front because of the dynamic nature of collaboration where people from different organizations collaborate dynamically toward achieving a goal. In the context of dynamic collaboration, when a person requests access to a resource, the decision to either grant or deny is based on trust. This section discusses how trust is integrated into the SCODA model in dynamic collaboration. The concept of trust is discussed first and its general characteristics are presented. Security deals with the concept of Risk. The relationship between trust and risk is explored. Finally, the role of trust and its context in the SCODA model is discussed.

6.7.1 What is Trust?

Trust is defined in similar terms in both the oxford dictionary [157] and in the online dictionary [158] as follows:

Definition: Trust

> *Firm belief in the reliability, truth, ability, or strength of someone or something* [157].
>
> *Reliance on the integrity, strength, ability, surety, etc., of a person or thing; confidence* [158].

From a human collaboration viewpoint, trust is a subjective notion and implies an individual's opinion of another. It could be based on evidence available to the individual. Also, trust is asymmetric in the sense that two individuals need not have similar trust in each other [159]. Numerous research disciplines have explored the concept of trust and how to design, implement, and reason about trust in an objective manner. In the social sciences discipline, the paper [160] describes trust as something a cognitive agent has with another agent in the context of goals and beliefs. An agent trusts another relative to a goal. In the words of the author *"Trust is a mental state, a complex attitude of an agent x towards another agent y about the behavior/action relevant for the result (goal) g."* When an agent X trusts another agent Y in the context of a goal "g", X has belief that Y will perform some action "α". The notion of delegation is implied in trust. Trust plays a key role in ecommerce. The specification of trust in such applications is discussed in [161]. The buyers must trust suppliers in their competencies, honesty etc., while the suppliers must trust buyers that they can pay for goods or services. In their model, the components of a trust relationship are: 1) trustor – subject that trusts a target entity

trustee, 2) trustee, 3) a specific context with associated level of trust, and 4) the conditions under which this relationship becomes active. The authors define trust as a quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context. Trust is not symmetric, so this belief by the trustor does not imply any similar belief by the trustee. They developed a specification notation called SULTAN (Simple Universal Logic-oriented Trust Analysis Notation) to specify, analyze and manage trust relationships for Internet applications.

There is no universally accepted definition of what trust is or how trust should be managed [162]. It has been defined from the perspective of social sciences and cognitive psychology, e-commerce, business management, etc. The attributes associated with the notion of trust include reliability, competence, dependability, availability, honesty, truthfulness and security. The characteristics of trust relevant for this research in the context of onboarding collaboration are as follows:

- trust is a relationship between two or more entities.
- trust is not a symmetrical relationship between entities.
- there are different levels or abstractions of trust relationships in the context of an enterprise, and inter-enterprise collaboration.
- trust is context sensitive.
- it is governed by conditions under which the trust relationships become active.
- trust and risk are integral to making access control decisions.
- trust evidence in dynamic collaboration build over a period of time and is used to make access control decisions.

This research considers trust in the context of collaboration and defines it as follows:

Definition: Collaboration Trust

Quantifiable relationship between trustor and trustee entities; it includes actions allowed on the shared resource and the associated risk.

This notion is captured as follows:

Collaboration trust is an ordered tuple: CT (Trustor, Trustee, Resource, Actions, Risk).

6.7.2 Risk vs. Trust

This research has discussed the notion of risk in the context of security. Security can also be viewed as risk management because the goal of security is to essentially protect information assets while risk analysis provides insights into the costs associated with breach of protection like accidental or malicious leakage of confidential information, denial of service, etc. When an entity trusts another entity the assumption is that the trustee is expected to behave in a certain way to execute the actions. For example, consider collaboration between sales organizations in acquirer company A and Company B, the company being acquired. Their collaboration requires sharing of sensitive information such as top customers, sales processes, etc. The expected behavior in this collaboration is that people from both companies would not divulge such sensitive information to anyone outside of this collaboration team. Risk quantifies the negative consequences if this expected behavior is compromised. The SCODA model proposed in this research integrates security in all phases and takes the view point that when trust relationships are defined they must also include the risk so that the appropriate dynamic access control decisions can be taken.

6.7.3 Trust taxonomy in Onboarding

Collaboration occurs at different organizational layers, both within an enterprise and across inter-enterprise domains. Accordingly the trust relationships must be defined to model these types of intra-enterprise and inter-enterprise collaborations. This research has identified the following types of trust relationships:

- intra-enterprise peer to peer trust between employees of the same functional unit.
- intra-enterprise trust between peers of the same organization within an enterprise.
- inter-enterprise peer to peer trust within the context of same functional unit.
- inter-enterprise peer to peer trust between the enterprises at the organization level.
- *community trust*.

For the purpose of this research two key trust abstractions, *strong trust and weak trust* are defined in the context of onboarding:

1. For two entities, X and Y in a collaboration strong trust is denoted by

   X $\leftrightarrow$ Y; where X and Y belong to the same company

2. For two entities, X and Y in a collaboration, weak trust is denoted by

   X $\longleftrightarrow$ Y; where X and Y belong to the two different companies

Consider a set of two entities: {X, Y}. Consider an entity Z which requests access to collaboration space shared by X and Y. The possible trust relationships are:

Case 1: X ⟷ Y; Y ⟷ Z ; implies X, Y and Z belong to the same company

Case 2: X ⟷ Y; Y ⟷ Z ; implies X and Y belong to the same company; Z is in the other company and Y and Z have a weak trust relationship

Case 3: X ⟷ Y; Y ⟷ Z ; implies X and Y belong to different companies; Y and Z belong to the same company

Case 4: X ⟷ Y; Y ⟷ Z ; implies X, Y, and Z belong to three different companies; useful in the context of a three way M&A (not considered in this research)

The strong and weak trusted relationships modeled are level 1 trust relationships based on whether the collaborating entities are within one company or they are from different companies. The concept can be extended further by considering other attributes like, for example, if the entities belong to the same functional unit with a company or not. These additional dimensions will lead to different levels of abstraction for trust relationships. Cases 1, 2, and 3 are useful for understanding how trust is handled in the SCODA model. For simplicity, an entity represents a collaboration team member for the rest of this discussion.

6.8 Trust Management in the SCODA model

6.8.1 In the context of onboarding, these trust relationships must be defined for better security management. The emphasis of this research is on illustrating the importance of trust management in onboarding where there is dynamic collaboration. Apriori, as discussed earlier, it is not possible to define access control policies statically in the dynamic environment of onboarding lifecycle. New teams form dynamically, team members are added and deleted, new documents are published in the repository, and sometimes team members need access to resources and documents dynamically for which no access control policies have been defined earlier. In this context, defining trust relationships will facilitate streamlining of access control decisions. The rest of the section illustrates how trust can be addressed in the various phases of the SCODA model. The discussion emphasizes the role of trust and it provides high level guidance to teams in terms of managing access in dynamic collaboration. For the purpose of this research and to facilitate the trust management discussion, only two levels of trust, strong and weak trust, have been defined in narrow scope. In practice, the teams could use the discussion presented here as a basis to extend the trust model that better suits their dynamic access control management needs in onboarding. Finally, an illustrative example of how trust is used in dynamic access management in onboarding is presented in section 6.8.2.Create Phase

Trust management is initiated in this phase of the SCODA lifecycle. Collaboration teams are formed and information assets are put in the collaboration repository. The trust relationship cases 1, 2 and 3 guide the automatic assignment of trust relationships among the collaboration team members. By default, there will be strong trust relationships among members of the same organization while weak trust relationships are automatically assigned to inter-enterprise relationship between the collaboration team members.

6.8.2 Operate Phase

In this phase, the following events must be addressed by trust management:

- A member requesting to be added to collaboration team
  The activities shown in Figure 6.7 (add participant) in section 6.6.2 is applied with the additional task of creating new trust relationships among all participants.
- A member deleted from collaboration team
  Trust relationships must be updated so that there are no trust relationships pointing to the deleted team member. The rest of the activities of the Operations Phase when a member is deleted are executed as discussed in section 6.6.2.
- Another collaboration team member requesting access to some information asset that has been designated for dynamic access

  This situation occurs because after a collaboration team publishes its information assets, members of other collaboration teams may sometimes need access to these assets in the context of their responsibilities. It should be noted that the members requesting access are not being added to the team; they are just requesting access to specific information asset. Granting access is determined by the following factors:

  1) Requesting team member must have a trust relationship with at least one of the members of the collaboration team,

2) The collaboration team member who has the trust relationship must sponsor the requestor,

3) The collaboration team votes either to grant or deny access,

4) Requestor gets notified,

5) Relationship between the different collaboration teams noted from a lesson learned perspective.

Consider the following example to illustrate the case of dynamic access control based on trust relationships. Table 6.1 shows the onboarding collaboration roles for company 1 (C1) and company 2 (C2) (acquired company). The following trust relationships are in place to begin with:

Collaboration_Trust_rel (Bob, Sarah) because they both have responsibility for finance domain. Let this team be named Coll_team_Finance. This is denoted by:

Bob ⟷ Sarah

Collaboration_Trust_rel (Mary, John) because they both have responsibility for Legal domain. Let this team be named Coll_team_legal. This is denoted by:

Mary ⟷ John

Trust_rel (Bob, Mary) because they both belong to same company. This is denoted by:

Bob ⟷ Mary

Trust_ rel (John, Sarah) because they both belong to the same company. This is denoted by:

John ⟷ Sarah

Table 6-1: Onboarding collaboration assignment

Emp	Company	Ent. Role	Coll Role	Content domain
Bob	C1	Finance	Principal Finance	Finance

			Lead	
Mary	C1	Legal	Principal Legal Lead	Legal
John	C2	Legal	Legal	Legal
Sarah	C2	Finance	Finance	Finance

Now let us assume that John in company C2 would like to access the finance data which happens to be an information asset held in collaboration team responsible for financial data of which Bob and Sarah are the team members. Since he does not have access to this data he needs to go to his trusted relationship with Sarah and request her to sponsor him for access to the finance data. If Sarah agrees to sponsor him then she will bring up this request to her community which will vote on the request.

6.8.3 Dissolve

In this phase, the emphasis is on deleting the trusted relationships established in the context of the collaboration team, and updating the trusted relationships repository so that for future endeavors of onboarding new insights are available for relationships that need to be established in the Create phase.

6.8.4 Archive

There is no direct activity related to trust management in this phase other than to archive the relationships that are established during the course of onboarding.

This section discussed the characteristics associated with trust and defined a trust taxonomy with reference to onboarding. It has formally defined the concepts of strong trust and weak trust which reflect intra company trust and inter-company trust among collaboration team members. Additionally, the section has discussed how dynamic trust

management is integrated into the SCODA model. The next section discusses how dynamic collaboration can be viewed as a self-organizing system so that as knowledge is acquired during the course of onboarding, the access control management system integrates this new knowledge for further access control decisions.

6.9 Self-Organization in Dynamic Collaboration

That Systems are large and complex is an observation made by researchers since the beginning of time as we know it. In the 1950s there was a concerted effort to design a general systems theory to understand the large and complex systems [163]. General systems theory attempts to formulate a theory which abstracts the discipline-driven theories like the theories in biology, physics, chemistry etc. [164]. Self-organization has been actively studied in the context of systems theory. Since then self-organization has been recognized as a pervasive phenomenon and has been used to study simple physical and chemical systems to large and complex social and cultural systems [165]. The concept of self-organizing systems is difficult to define precisely because a given system may be viewed as self-organizing at one level of abstraction while it may be viewed otherwise at another level of abstraction. Intuitively, self-organization suggests systems that appear to organize themselves without external direction, manipulation, or control [166]. Self-organization has been defined as a process in which the internal level of organization of a system increases automatically without being guided or managed by an outside source [167]. In cell biology it has been defined as the capacity of a macromolecular complex or organelle to determine its own structure based on the functional interactions of its components [168]. Common characteristics of the self-

organized systems studied are the complexity and dynamicity of the problem domains. Computer Science and IT enabled systems use self-organization as a modeling tool to understand the requirements of complex internet-driven applications and design solutions that are self-organizing. This is because it is impossible to know apriori all the possible interactions, relationships, and outcomes in the complex environment of inter-enterprise collaborations which are geographically spread. Self-organization has been investigated in information security (as discussed in the literature survey in this thesis) in managing access in ad hoc networks, distributed management of contextual data etc. Case studies of self-organization in computer science are discussed in [115]. The dynamic collaboration that this research discusses has the characteristics of self-organizing systems. The rest of the section presents general characteristics of self-organizing systems, and the characteristics of trust based dynamic collaboration. This leads to a comparative analysis of common features of self-organizing systems and dynamic collaboration. Finally, it discusses the application of self-organization in SCODA model.

6.9.1 Characteristics of Self-Organization

Many disciplines have studied self-organizing systems. A summary of characteristics of self-organizing systems discussed in the literature are the following [169]:

- The appearance of structure or a pattern without any external agent imposing it. An example is the crystallization where there is an appearance of symmetric patterns from a random collection of molecules. It is as if the system of molecules knows how to arrange itself into some ordered pattern.
- A multitude of initially independent components that end up working together in some cohesive manner. An example is neural networks where all neurons work independently but are also connected and together make sense of the input to

the brain. Another example of collective behavior is found in the animal world of herds and swarms.

- Absence of centralized control. For example, there is no centralized control in the brain and the connected neuron network makes the decisions collectively.
- Adaptation to changing environment. Examples of this include biological systems, adaptation to environment changes, etc.
- Global Order from local interactions. An example in physics is the scenario of magnetization where it is shown how a dis-organized set of magnetic pins becomes organized at cooler temperature.
- Distributed control. The brain is an example of distributed control. Though there are specialized regions of the brain no region is responsible for the overall functioning of the brain.
- Positive and Negative feedback. Magnetization is an example where under the influence of external magnetic field has influence on the spins of the magnetized iron which align themselves according to the strength of the magnetic field.
- Dynamic. An example of this from the business world is where markets correct themselves based on numerous financial factors.
- Internal level of organization of a system increases automatically without being guided or managed by an outside source.

6.9.2 Characteristics of Dynamic Collaboration

The dynamic collaboration in onboarding exhibits the following characteristics

- Apriori, one cannot conceive of all possible configurations, purposes, or problems that the collaboration environment may be confronted with.
- Access control decisions cannot be pre-determined completely at the beginning of the onboarding lifecycle.
- Access control decisions are made independently by various collaborating teams.
- There is a feedback loop into the access control system as and when new access control decisions are made by independent collaborating teams.

- There is a feedback loop into a knowledge gathering system for future instantiations of onboarding collaboration.
- Adaptation of access control by various participants throughout the onboarding lifecycle.

In essence the dynamic collaboration in onboarding exhibits many similarities in characteristics with respect to self-organizing systems. Self-organizing systems theory provides a perspective for studying systems and for designing, building, and controlling systems. A critical component of any such system is the concept of feedback and learning. As the system evolves, the knowledge gained from a collection of independent but co-operating entities is fed into a global repository which in turn facilitates new structures and processes in future instantiations. The next section illustrates self-organization in the SCODA model.

6.9.3 Self-organization in SCODA Model

The inter-enterprise onboarding collaboration displays all the characteristics of self-organizing systems described in the previous section. The following activities reflect the self-organization in the SCODA model:

- Create Phase

  In the create phase, the self-organization principle of “seeding” the initial system is applied in terms of creating the necessary roles, responsibilities, collaboration relationships, adding information assets to the repository, and setting up access control policies. From the perspective of an “observer”, the system appears to be organized to begin with, as some self-organization researchers claim is a necessary aspect of such systems.

- Operate Phase

It is in this phase that all characteristics of self-organizing systems are observable. The dynamicity of the system is reflected in the interaction and changes in terms of adding and deleting members, establishing new spontaneous collaborative relationships, creating new access control paths through community based decisions, the positive and negative feedback provided in the context of community based access control decisions, the distributed access control decisions of multiple collaboration teams and finally the knowledge assimilation of dynamic changes to the global access control framework.

- Dissolve Phase

  The self-organization is evident in this phase when collaboration teams dissolve. There is dynamic change in terms of terminating roles, entities, and access to information assets. These changes are propagated throughout the other collaboration teams which subsequently organize themselves in terms of available relationships and paths to information access to continue the onboarding.

- Archive Phase

  In this phase, it is not evident as to how the concepts of self-organization apply. One of the reasons that the perspective of self-organization is not applicable in this phase is that archiving is not a concept associated with self-organizing systems. For natural self-organizing systems such as the stars, galaxies, biological systems there is no “end-of-life” state and they are in a state of organization in perpetuity.

This section has shown how self-organization is a perspective that one could apply to understand the dynamic collaboration in onboarding. Perspectives, paradigms, models, etc. facilitate understanding of problem domains in well-defined abstractions and concepts. This in turn will enable the design, development, implementation, and operations of systems, a majority of which are driven by software in today’s world. One

of the important aspects of such environments is *change*. Change is an integral component of any enterprise. As an enterprise continues to operate, there will be changes in people, business processes, technologies etc. The next section discusses change management in the context of the onboarding lifecycle.

6.10 Change Management in Onboarding

The theoretical foundations of change management were based on the mathematical branches of theory of groups and theory of logical types [170]. These theories explained first order and second order changes. The first order changes focused on improving the processes and procedures of existing systems, while the second order changes focused on activities when the system itself is changed. For example, shifting the strategic focus of a business, or automating business processes is a first order change. An example of second order change is the process of withdrawing money from an ATM, ordering books online, etc. As the literature evolved new theories were proposed in between the two extremes of the first order and the second order. In addition, theories from psychology, sociology, etc., were combined to propose new change management perspectives which considered attributes such as motivation in an individual's behavior [171].

In the context of onboarding acquisitions, change management deals with changes at an enterprise level as well as changes within the context of dynamic collaboration itself. At the enterprise level changes occur in terms of assimilating and integrating the acquired company's people, processes, technologies, customers, partners, and vendors. One of the key aspects of change management is not just the change itself but

the pace of change that can potentially inhibit successful onboarding [172]. Change management is viewed as a process by which an organization gets to its future state, its vision. While traditional planning processes delineate the steps on the journey, change management attempts to facilitate that journey. The main focus of change management in this research is about how to manage changes in dynamic collaboration. These changes encompass changes in roles, responsibilities, access control policies, etc., during the dynamic collaboration in onboarding. Change management in this context must also capture the lessons learned from a continuous process improvement perspective. A secondary focus is to provide insights into change management at a holistic level of enterprise level integration of an acquisition. This will provide a context to the change management discussion in the SCODA model.

6.10.1 Enterprise Level Change Management in Onboarding Lifecycle

Change is constant. Organizational change management is an approach that an enterprise adopts to ensure that changes are implemented in a well-defined manner and that they have long lasting benefits. Management researchers, behavioral and social scientists, and researchers in software engineering, information systems, computer science, and information technology continue to investigate the topic of change management. There are many enterprise change management models proposed in the literature such as Kotter's eight steps to change [173], Bridge's transition model [174], Roger's five step process for technology adoption [175], Kubler-Ross change curve model based on the five stages of the grieving process [176], Prosci's ADKAR model [177]. Change management at the enterprise levels deals with changes in: 1) processes, 2) systems, 3) organizational structures, and 4) job roles. The

main objective of change management is to move a company from its current state to a future state that is aligned with the business strategy. To make the change there should be a structured set of activities. Project management provides the tactical structure to make the change happen. At the enterprise level change management initiatives, project management focuses on the tasks while change management focus on the people that are impacted by the change [177]. Figure 6.9 depicts components of change management in onboarding. It reflects onboarding acquisitions because it takes the company from an existing state to a future state in a systematic way through an onboarding lifecycle that includes both project and change management.

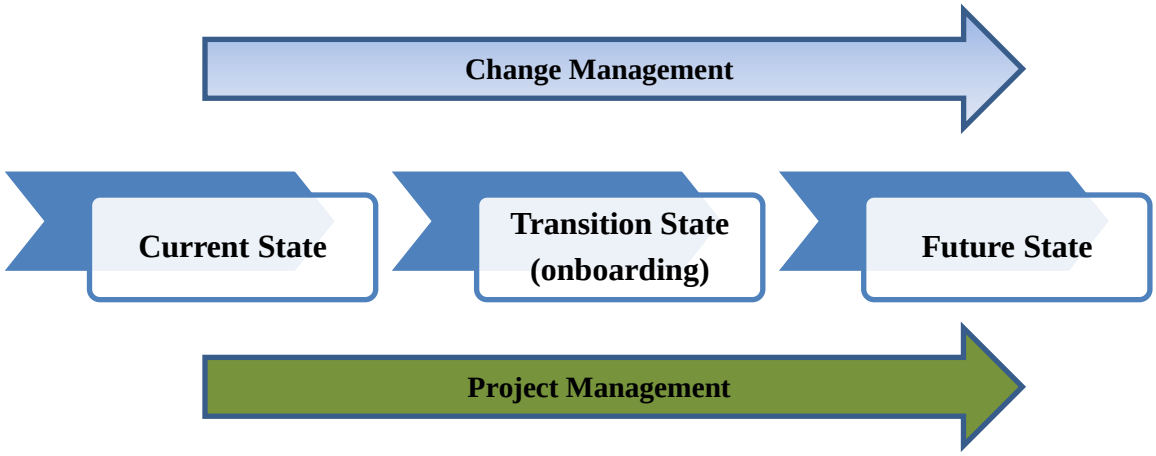


Figure 6-9: Change management components in onboarding

This research views change management in onboarding with different semantics than what the author defines in [177]. The semantics attributed to change management include the impact of changes during the onboarding lifecycle in roles, responsibilities, access control, knowledge assimilation and feedback into the collaboration knowledge vault, etc. In other words, change management, as discussed here, is not about people management only, as suggested in [177]. This research viewpoint of change

management is prevalent in adopting technology solutions [7]. The next section discusses details of change management in dynamic collaboration in onboarding.

6.10.2 Change Management in Dynamic Collaboration

Figure 6.10 shows a domain model of onboarding an acquisition which includes collaboration teams, an information assets repository, a project management office, a dynamic collaboration learning system, a publish and subscribe system, a trust management system, and a security management system.

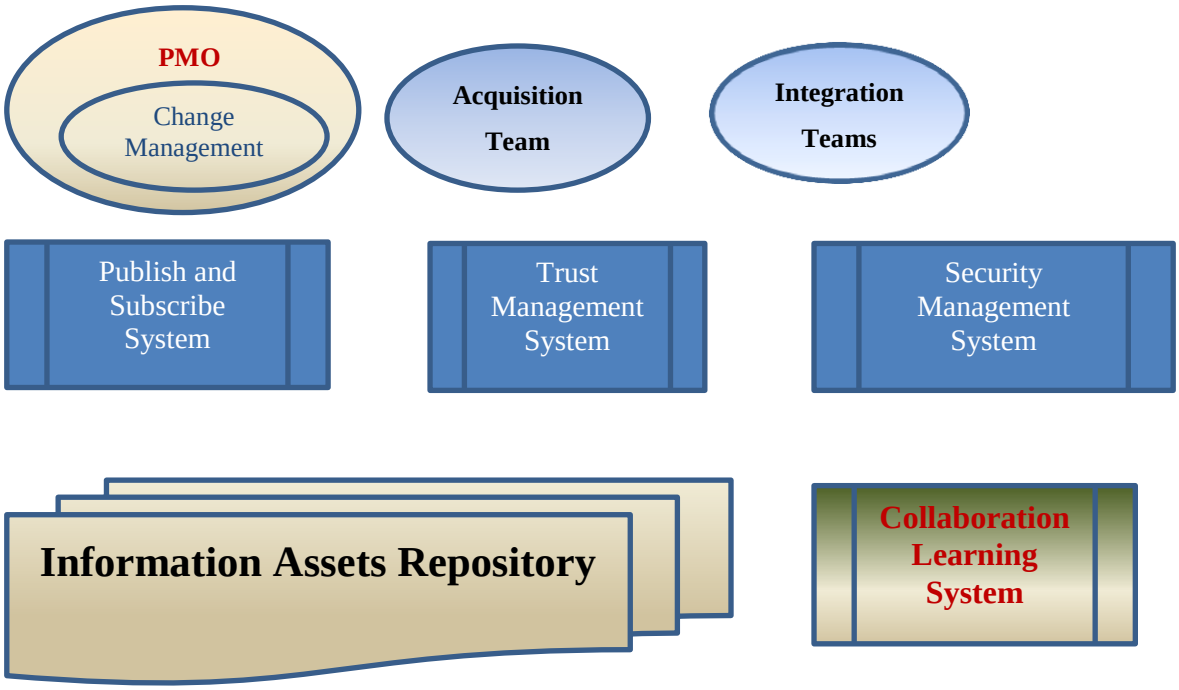


Figure 6-10: Domain model of onboarding collaboration

The Project Management Office (PMO) is responsible for project execution. They are responsible for maintaining the overall project plan for all onboarding activities and for managing change from the perspective of maintaining information about resources,

timelines, deliverables, team communications and executive communications. In essence they are responsible for coordination, communication, and facilitating cooperation among all onboarding participants.

The collaborating teams themselves will deal with change during the onboarding lifecycle. When new roles are created or existing roles are modified, this new information is transmitted to the collaboration learning system. In addition, when a collaboration team makes a dynamic access control decision using the trust management system, this information is also updated in the collaboration learning system. When a participant leaves a team, the access control management system is accordingly updated. When a collaborating team either adds or deletes information assets this information is transmitted to the collaboration learning system. In addition, if a team identifies an information asset as available for dynamic access control, this information is transmitted to the publish and subscribe system so that other teams become aware of the newly added information assets. In a nutshell, this briefly describes the interaction between the various components of the onboarding collaboration domain model. Change management is integral to the overall access control management in onboarding collaboration. Instead of being prescriptive in its discussion, the objective here is to raise the awareness of the importance of change management in ensuring security across the entire onboarding lifecycle.

6.11 Summary

This chapter has presented a new access control model that emphasizes building security across the entire onboarding lifecycle. To begin with, it defined an onboarding collaboration model SCODA that every onboarding collaboration team should follow. In

this model, every collaboration team goes through a process lifecycle of: Create Operate, Dissolve, and Archive. It defined the concepts of enterprise, functional and collaboration roles as a means of addressing security. Next it discussed how security is addressed in all these phases of collaboration through the necessary algorithms. Trust and Risk are integral to security. This chapter defined and discussed how these are incorporated in managing security in dynamic collaboration to determine access dynamically through community trust. A key idea presented in this context is the importance of collaboration teams identifying information assets that are released for dynamic access. The chapter defined the concepts of strong and weak trust and discussed how these apply in determining dynamic access to information. The role of self-organization in understanding dynamic collaborations is discussed and it is shown that onboarding collaboration shares similar characteristics with self-organizing systems. Finally, the chapter presents a discussion on change management and further shows how change management is viewed from the perspective of this research.

7 Model Validation and Update

"The expert knows more and more about less and less until he knows everything about nothing."

-- Mahatma Gandhi

7.1 Introduction

Verification and Validation are concepts extensively discussed in the computer science domain. They are independent procedures for checking that a product, system, model, or a service meets the requirements and specifications and that it fulfills its intended purpose [178]. The Project Management Book of Knowledge (PMBOK) guide, an IEEE standard, defines validation and verification as follows [179]:

> **Validation**
> *The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance by and suitability for external customers.*
>
> **Verification**
> *The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process.*

In practice, validation is associated with the question: *are you building the right thing?* And verification is associated with the question: *are you building it right?* In addition, these two terms are often used interchangeably. In the literature, the terms verification and validation are sometime preceded by the term "independent" to signify that these are performed by disinterested/independent third parties. This independent verification and validation is often denoted by the acronym IV&V. In the context of this research the proposed approach and model was subject to expert validation which resulted in further

refinement. Expert validation was the chosen method because it provided an opportunity for numerous people associated with executing mergers and acquisitions such as M&A facilitators, business stake holders different functional units, IT architects, and Integration experts to review the proposed approach and model from the perspective of addressing collaboration security in onboarding an acquired company. The rest of the chapter discusses the details of expert validation.

7.2 The Validation Method

The new approach and model proposed in addressing access control in onboarding is of practical significance because of its intended usage in onboarding acquired companies. As a result, it was deemed appropriate to solicit review and feedback from industry experts to validate the proposed solution. It was further determined that at least five to seven experts who have experience in different aspects of onboarding are appropriate for providing the review and feedback on the proposed approach and model. The process used for validating the model with the experts is the following:

1. Identify the validation experts

   The list of survey participants was analyzed to identify experts with backgrounds in different aspects of onboarding. The selected participants included people who managed acquisitions, integration planning, IT architects, security experts, academic professionals who are experts in process modeling, and business stakeholders involved in onboarding acquisitions. As discussed in Section 7.4, a total of 10 experts were selected.

2. Email the thesis to the experts.

The experts' tasks were the following:

   - Read the abstract to get an overview of the research
   - Review the approach and the model discussed in Chapter 6
   - Provide feedback, comments, and suggestions for improvement
   - Optionally read the other thesis chapters and provide any other feedback if they wish

3. After one week, reached out to the experts to set up in person meetings
   - The meetings usually lasted between 1 and 2 hours on average.
   - The experts usually commented on the overall scope of the research, the structure of the thesis, the research methodologies and methods selected
   - The experts provided specific feedback solicited vis-à-vis the approach and model as discussed in Chapter 6.
4. Once the model was refined based on the experts' feedback, one final review was carried out by three experts and they have concurred with the refinements.

The model was first validated with two experts which resulted in preliminary refinement. It was further validated with ten experts and resulted in further refinement. The rest of the chapter details the validation efforts, feedback from the experts in the industry, and the final refinement of the approach and the model.

7.3 The First Refinement

The approach and model was evaluated by two researchers whose expertise is in business information systems, process modeling, and Total Quality Management (TQM). The reviewers' feedback included the following key observations:

- The SCODA model as shown in Figure 6.2 in Chapter 6 signifies unintended sequential flow from archive phase to create phase where the semantics of the flow is not well defined.
- The "archive" phase discussion implies incorrectly that each team is doing its own archiving of data after the team's work in onboarding is complete
- The discussion in Chapter 6 implies that the output of this research and the processes and models described should together be labeled as "approach and model".

Figure 7.1 reflects the changes to the SCODA model based on the input from the first set of experts. It shows that every team during onboarding collaboration goes through the phases: 1) create, 2) operate, 3) dissolve, and 4) archive. The archive phase activities are more clearly defined in the final refinement discussed in Section 7.5.

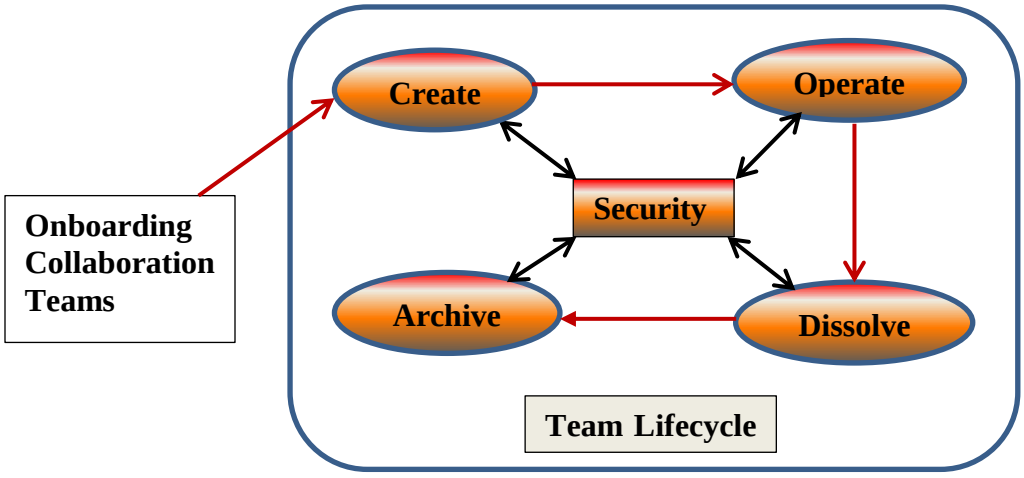


Figure 7-1: SCODA Model: First Refinement

7.4 The Experts Feedback

The approach and model as discussed in chapter 6 was subjected to expert review in the industry. A total of ten experts were included in the review. The roles played by these experts in onboarding undertakings included two industry experts in mergers and acquisitions, two integration leaders, three functional leaders in marketing, vendor management, and partner management respectively, product development and engineering leader, three enterprise architects, two business leaders, and three IT architects.

The feedback, observations, and comments gathered from these expert reviews are as follows:

1. Information dissemination and declassification occurs during onboarding. In addition, information travels at different speeds and to different levels of stakeholders. During this process, the sensitivity of information changes. This characteristic could perhaps be reflected in the activities associated with the phases: create, operate, and dissolve.
2. The SCODA model as depicted in Figure 6.2, Chapter 6, could be redrawn to show that each team goes through the stages of creation, operation, dissolution, with archiving coming as a last step where a designated team member will be responsible for initiating archiving of team artifacts.
3. The archiving is not the responsibility of each of the teams. Instead, they initiate the process of archiving artifacts as the last activity where perhaps a designated IT team is responsible for performing the activities of archiving and restoring data.
4. The acquisition team is alive until the acquisition integration is complete.
5. There can be multiple integration teams during onboarding.

6. The model could in the future be generalized beyond acquisitions onboarding. In the general context the terminology could be changed to reflect two roles: 1) a role to reflect an existing entity, and 2) a role which represents an entity joining an existing entity.
7. Show the activities reflecting that SCODA is self–organizing by depicting a feedback loop and monitoring.
8. Specify who is responsible for archiving and monitoring of the archive.
9. The trust levels should include at least one more level to characterize the scenario within the same enterprise where collaboration members belong either to the same functional unit or different functional units.
10. Voting is an interesting idea but most often the team leader decides access rights in today's environment. However, tying the concept of risk in making access control decisions dynamically should be explored as it speeds up decision making.
11. Mapping acquired company roles to acquiring company's role is an important activity in determining access control.
12. There is a philosophy of "learn as you go" in integration. As a result the access control policies and decisions do change dynamically.
13. New data is constantly generated during the onboarding as both companies are still operational. So, access control policies are constantly updated.
14. HR data access control policies are imposed by external security standards, while the business data access control policies are dictated by policies at the company level and easily controllable.
15. Securing historical data is another facet of onboarding an acquisition.

The feedback has provided insights into some of the issues that need to be addressed in the context of this research and in future work to enhance the applicability of this research in the general subject area of dynamic collaboration in other contexts. In the

next section, the updated approach and model based on experts' feedback is presented.

7.5 The Final Refinement

Three aspects of the approach and model are refined based on experts' feedback and suggestions: 1) refinement of the SCODA onboarding collaboration process model, 2) the activities associated with the four phases of the SCODA model, and 3) extending the trust taxonomy to model two different types of trust relationships in an enterprise. The details of these three refinements are presented in this section.

7.5.1 Updated SCODA Onboarding Collaboration Process Model

Figure 7.2 depicts the updated SCODA model.

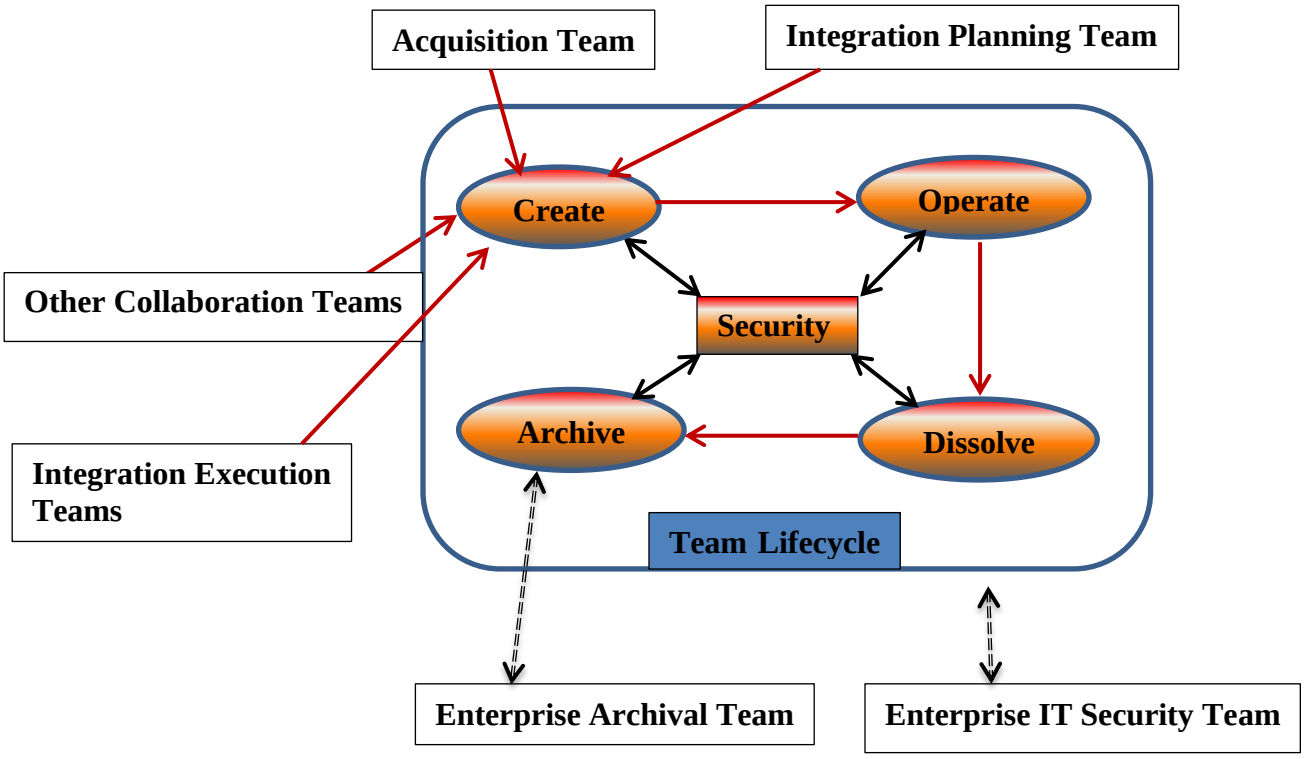


Figure 7-2: Updated SCODA model

The key aspects of the model are as follows:

1. The Acquisition team is called out to reflect the fact that this is a team that has the longest persistence in the entire onboarding lifecycle.
2. The Archive Team is called out because it is responsible for all archival activities. In the archive phase, the team member responsible for archiving the team artifacts will work with the archival team which is a central resource.
3. The Security team is called out to reflect the fact that all collaboration teams must address security and they need to collaborate, cooperate, and coordinate with the security team.
4. The Integration Planning team is called out since they are responsible for the overall integration planning and they also project manage multiple streams of integration execution teams.

7.5.2 Building Security in CODA (Create, Operate, Dissolve, Archive)

The experts' feedback resulted in updating the activities in each of the phases of the SCODA model. The details are the following.

7.5.2.1 Building Security in Create Phase

The updated activities in the create phase are shown in Figure 7.3. Data classification acquires importance in the context of dynamic access control management in onboarding collaboration. Data classified as subject to *outside the enterprise policies*, for example the human resources data regulated by federal and health care standards, is not something that would normally be assigned access automatically based on trust and voting schemes. Instead, when one requires access to such information, they may

have to submit their request to information security office and follow the corresponding policies and procedures.

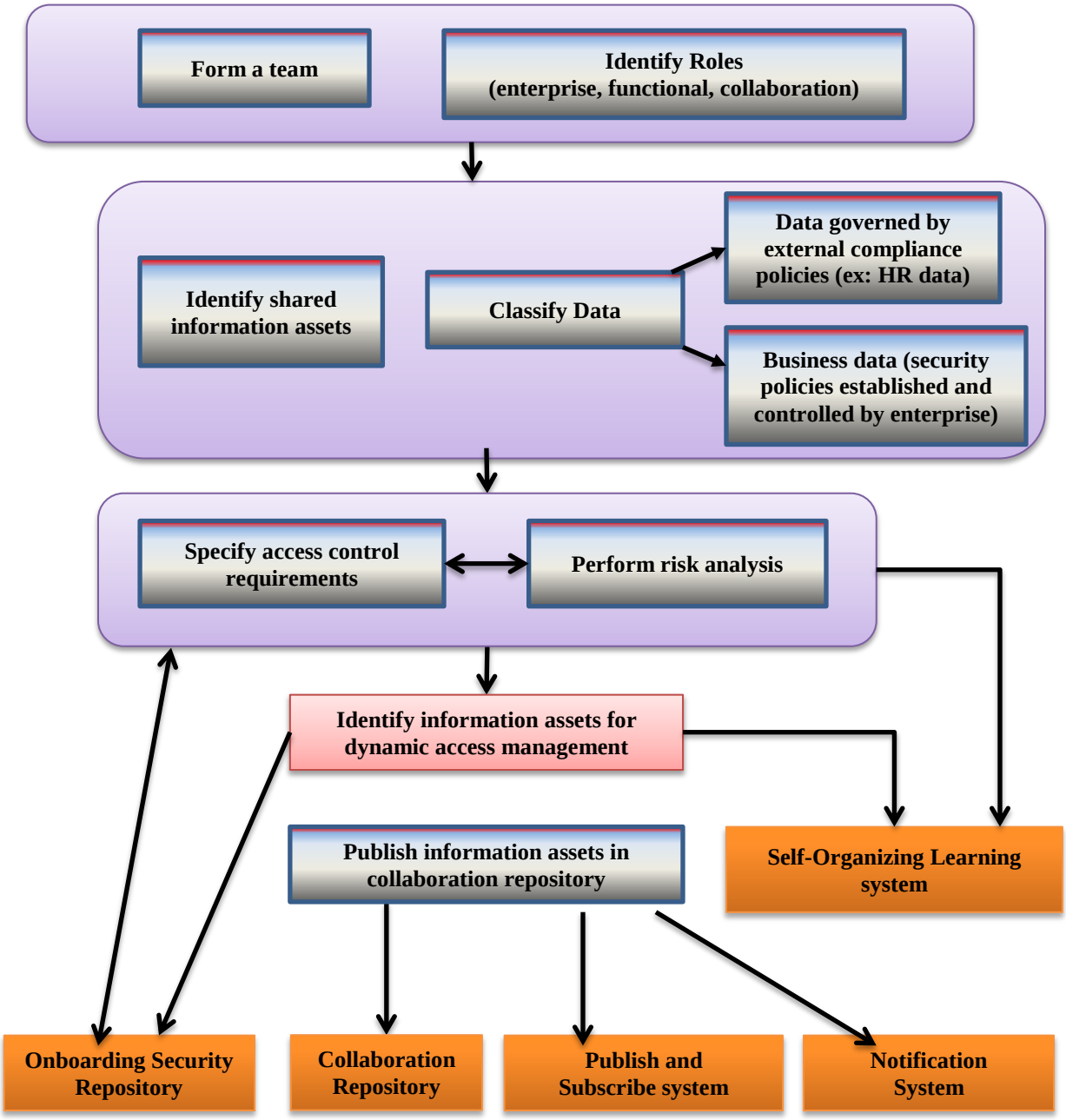


Figure 7-3: Security in create phase

It should be noted that the proposed model does not impose this restriction. It just suggests that this type of information requires closer scrutiny in terms of dynamic access control. The onboarding security repository will include all information pertaining to enterprise, functional, and collaboration roles, their access information, the information subject to dynamic access based on trust, and policies and procedures to grant access to information assets that could be requested during the onboarding collaboration.

7.5.2.2 Building Security in Operate Phase

In the operations phase, while the team is actively working on the onboarding tasks, additional data is generated, new information resources are added, new members may be included in the team, etc. It is imperative that access control be formally addressed for these dynamic scenarios where there is constant change in data and other resources, changes to team, changes to roles etc. Figure 7.4 shows how the SCODA model guides the activities of publishing new data resource and/or changing security requirements for existing data resource. The experts' feedback helped in identifying that classification of data is an important element of addressing security in this phase. Another facet of operations phase is information distribution aspect as it ages over time and the risk associated with its dissemination changes. Over the period of onboarding collaboration, information is usually known to only a small set of people in the beginning stages and as the integration progresses, it is made available to the appropriate stakeholders and other participants. This implies that the onboarding security repository is constantly updated to reflect changed access control policies.

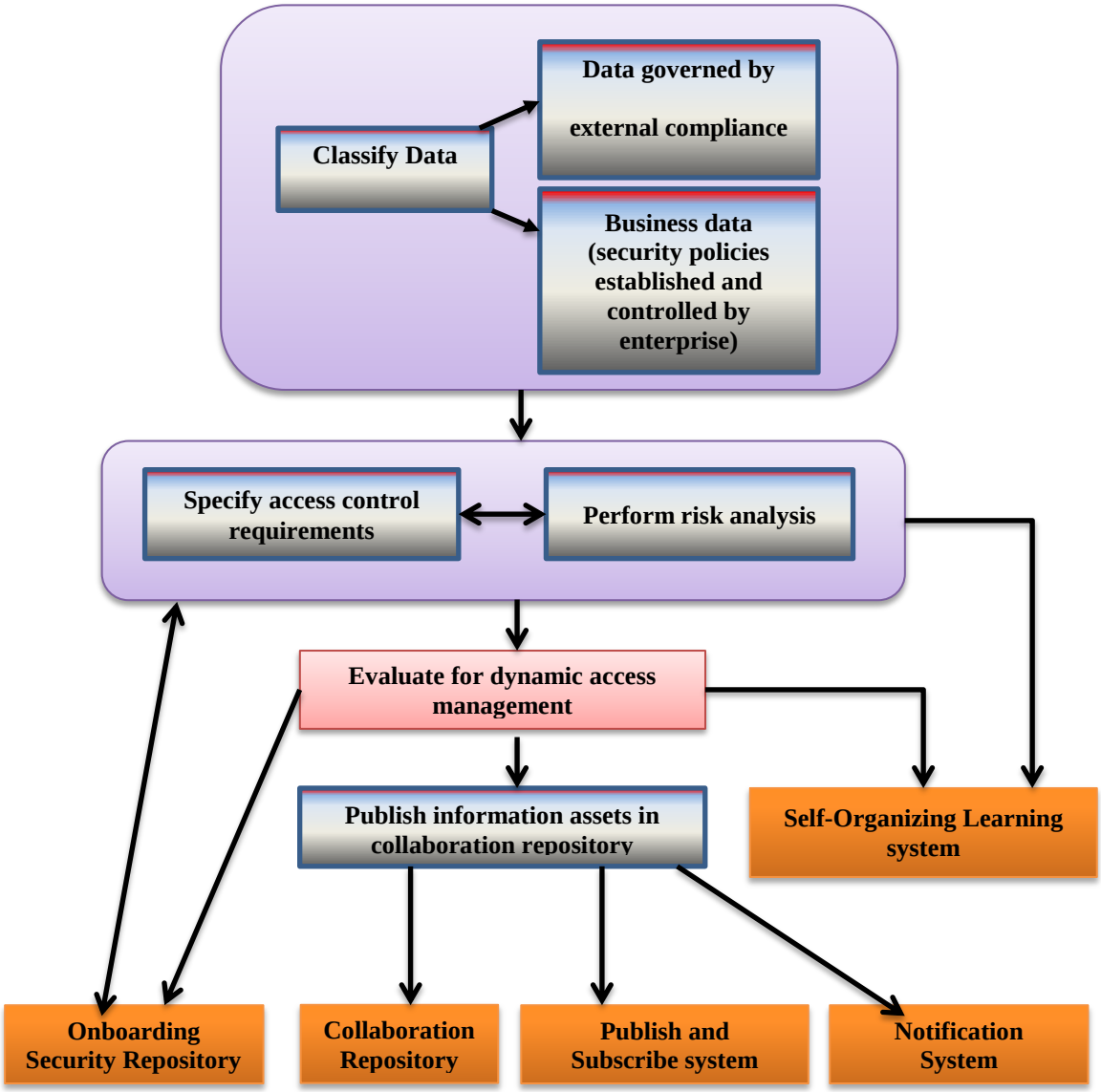


Figure 7-4: Adding a data resource and/or changing data security

Figure 7.5 shows essential steps in adding member to an existing collaboration team. In this case, the important aspects of security is to assign the appropriate enterprise, functional, and collaboration role, specify the trust relationship if new collaboration role is established, update the team roster, and notify participants. For simplicity, not all the globally available resources such as the onboarding security repository are depicted.

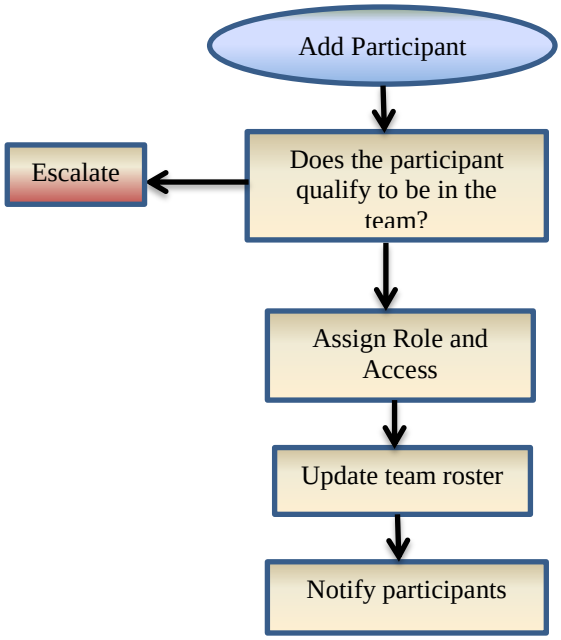


Figure 7-5: Adding a member to collaboration team

The activities in the dissolve and archive phase are similar. The key aspect in the dissolve phase is to identify a team member who will be the interface with the archival team. Once the archival request is sent to the appropriate entity/person, the team's access to the collaboration repository is disabled and the onboarding security repository is updated.

7.5.3 A Trust Taxonomy

The experts' feedback reinforced the ideas of this research that the concept of trust and risk are important considerations in dynamic access control in onboarding. The concept of strong and weak trust combined with assessment of risk in granting access is a viable option in access control in onboarding collaboration. The suggestion given by experts is to enhance the trust taxonomy to include three levels:

1. Strong Trust – between collaborating team members within an enterprise where they belong to the same department or functional unit.
2. Medium Trust – between collaborating team members within an enterprise and they belong to different departments/functional units.
3. Weak trust – between collaborating team members who belong to different enterprises, one the acquiring company and the other is the company that is being acquired.

This research accepts these recommendations. However, it should be noted that the key aspects of trust and risk proposed in this research is not prescriptive in nature. Different organizations can adapt the notions of trust taxonomy and risk discussed here to suit their needs in implementing access control in onboarding.

7.6 Summary

The experts review and their feedback validated the new approach and model discussed in this research. They agreed that this research will lead to a systematic approach in managing security in onboarding companies. The constructive feedback and suggestions provided the guidance to refine the approach and the model to better reflect the practice of onboarding collaboration in mergers and acquisitions. The critical aspect of security suggested by experts included the notion of data and information classification based on the externally guided security policies and the business driven policies. This distinction provides insights into determining the information assets that may be candidates for dynamic access management without pre-defined security policies. Finally, the enhanced trust taxonomy will facilitate better modeling of dynamic access control based on risk.

8 Conclusions

"A journey of a thousand miles must begin with a single step." – Lao Tzu

8.1 The Journey

This research undertaking is a consequence of insights gained from many different sources. The work experience in the industry encompassing information security, onboarding, and change management has enabled the identification of possible gaps that need to be addressed in collaboration security. The literature review enabled the identification of relevant security issues in the realm of information security, dynamic collaboration, and onboarding. Detailed surveys with industry experts and practitioners further enabled narrowing of the research topic. It became clear that systematically addressing access control in onboarding is an important research area with both practical and theoretical implications. The pursuit has allowed for advancing the field of access control in dynamic collaboration and it enabled the formulation of an approach and model that could be adapted in the industry in the context of onboarding. The rest of the chapter presents the contributions of this research and future directions.

8.2 Research Contributions

This research is a step forward in systematizing access control in onboarding. It is also a step forward in formulating access control in the general context of dynamic inter-enterprise collaboration. The research began with understanding the characteristics of the problem in onboarding an acquired company. This is a typical scenario in mergers and acquisitions where a company acquires another company for numerous reasons

including expanding their market reach, complementing their solutions, gaining customers, and increasing revenues. The context is one of inter-enterprise dynamic collaboration. Though access control had been addressed by researchers and practitioners in dynamic collaboration, it has not been addressed in onboarding which provides a different perspective of inter-enterprise collaboration. Many business sensitive documents, processes and other artifacts are shared among collaboration teams belonging to different organizations and this engenders a security risk.

This research made the following key contributions in the context of onboarding:

1. Developed the SCODA secure onboarding collaboration process model to address security systematically. In this model, the team collaboration is viewed from the perspective of a lifecycle that includes four phases: create, operate, dissolve, and archive. The creation phase is when the team is formed; operation phase is where the team works on a collection of activities related to onboarding; dissolve is a phase where the team wraps up their collaboration and designates a person to archive the collaboration artifacts that the team shared; and archive is the phase where the designated team member collaborates with the onboarding security office and archiving team (typically an IT function) to bring a closure to the collaboration while ensuring that all information assets are safely archived, and access control to team members is disabled.
2. Developed a mechanism to address security as an inherent activity built into the lifecycle of dynamic collaboration in onboarding. The set of activities that

should be performed and the issues that need to be addressed in terms of access control in each phase are presented.

3. Integrated the concept of trust in managing access in dynamic collaboration. The taxonomy proposes three levels of inter-enterprise trust in onboarding which can be adapted by enterprises.
4. The concept of risk analysis is introduced in addressing dynamic access control. In this context, the research proposes that dynamic access control based on trust relationships is contingent upon identifying the risks associated with the information assets. Depending on the risk tolerance, these information assets could be made available for access dynamically without pre-defined static access control policies. Instead access for such information assets is granted dynamically based in trust relationships and community voting.
5. The perspective of self-organizing systems is presented as a way to gather feedback on secure access control during the onboarding lifecycle and update the collaboration security repository. This self-learning loop further enables dynamic access control.
6. Change management is addressed as an integral component of onboarding process.

In addition to these key contributions, the research introduced new ways in defining security requirements, enterprise, functional and collaboration roles, collaboration patterns, and reinterpreted access control requirements in collaborative sharing. The

next section discusses the possibilities of using this research as a basis for further contributions in both theory and practice of access control in dynamic collaboration.

8.3 Future Research

Any research undertaking usually results in identifying further scope for extending the research results in future endeavors in the chosen domain. It is also not unusual to seek possible adaptation of the research in other scientific, academic, and industry domains. In the spirit of this observation, there are several aspects in which this research could be pursued further.

One aspect of this research is that the new approach and model is not adopted or adapted widely though the industry experts have validated the model and unanimously agreed that this is a promising approach for them to use. There is valid scope to use this in numerous onboarding projects in the future. The resulting data from these undertakings should provide insights into enhancing the model and making it an integral component of enterprise architectures and security. Many organizations have enterprise security frameworks as part of their overall enterprise frameworks. It will be useful to extend this research to include these enterprise wide frameworks so as to provide one holistic and consistent framework to address all aspects of managing a business.

Dynamic collaboration continues to be an active research area. Grid computing based models of collaborations are actively discussed. From the literature review in this space, it is not clear how dynamic access control could be addressed systematically while not addressing data classification as discussed in this research. Trust management and

community based voting is another active area of research where the concepts of data classification, business driven policies, externally driven mandated policies must be integrated in proposing solutions. This is an area that will be investigated further.

Though this research context is onboarding, more specific areas of onboarding models can be considered in the future. For example, there are numerous scenarios such as a big company acquiring a small company, merger between two similarly sized companies, and a company acquiring another company that spans international boundaries.

Finally, the future research considerations may include the scenario of extensive data generation during long onboarding cycles while both the companies are operational. In this scenario, granting access to new information being generated dynamically in either organization is a topic that warrants further research.

9 References

[1] H. G. Barkema, "How do firms learn to make acquisitions? A review of past research and an agenda for the future," *Journal of Management*, vol. 34, pp. 594-634, 2008.

[2] D. M. DePamphilis, "Chapter 1 - Introduction to Mergers and Acquistions (M&As)," in *Mergers, Acqisitions, and Other Restructing Actvities*, Elsiever, 2010, pp. 3-46.

[3] "http://www.businessdictionary.com/definition/collaboration.html," [Online].

[4] National Security Telecommunications and Information Systems Security Committee, "National Information Systems Security (INFOSEC) Glossary," National Security Agency, 9800 Savage Road, STE 6716, Ft. Meade, MD, 2000.

[5] M. Siponen, "Designing Secure Information Systems and Software," University of Oulu, 2002.

[6] H. F. T. Micki Krause, Handbook of Information Security Management, CRC Press LLC), 2007.

[7] P. Chillakanti, "Role-based Information Security: Change Management Issues," in *ISICT- International Symposium on Information and Communication Technologies*, Las Vegas, NV, USA, 2004.

[8] Abdessamad I and et.al., "A Flexible Access Control Model for Distributed Collaborative Editors," *SDM 2009, LNCS 5776*, p. 89–106, 2009.

[9] B. Zhao, "Collaborative Access Control," Helsinki University of Technology, Helsinki, 2001.

[10] J. Jin and et.al., "Role-based Access Management for Ad-hoc Collaboration," in *SACMAT 2006: 11th ACM Symposium on Access Control Models and Technologies*, Lake Tahoe, 2006.

[11] G. Dai, "A REVIEW OF ONBOARDING LITERATURE," Lominger Limited, Inc., a subsidiary of

Korn/Ferry International., 2007.

[12] K. Rollag, "Getting New Hires Up to Speed Quickly," *MITSloan Management Review,* vol. VOL.46, no. NO.2, 2005.

[13] S. Mortvedt, "Formal On-boarding Procedures: An Implementation Model for XYX Company," 2009.

[14] K. Cashman, "Onboarding," *Leadership Excellence* , vol. 24, no. 4, 2007.

[15] J. Birkinshaw, "MANAGING THE POST-ACQUISITION INTEGRATION PROCESS:HOW THE HUMAN INTEGRATION AND TASK INTEGRATION PROCESSES INTERACT TO FOSTER VALUE CREATION," *Journal of Management Studies* , vol. 37, no. 3, pp. 395-425, May 2000.

[16] Aberdeen Group., "All aboard: Effective onboarding techniques and strategies.," Aberdeen Group. All aboard: Effective onboarding techniques and strategies. Retrieved 1211,, 2008. [Online]. Available: http://www.aberdeen.com/launchlreport/research ~reviews/4617 -RP-effectiveonboarding.

[17] E. Harmeyer, "On-boarding our new employees," [Online]. Available: http://www.rockwellcollins.com/horizons/volume 13 -issue41 onboarding/index.html.

[18] D. Lee, "13 questions to maximize your onboarding efforts," 2007. [Online]. Available: http://www.ere.net/2007/09/12/13-questions-to-maximize-your-onboarding-efforts.

[19] P. D'Aurizio, "Human Resource Solutions. Onboarding: Delivering the Promise," *Nursing Economics,* vol. 25, no. 4, pp. 228-229, 2007.

[20] A. Killen, "Integrating Acqusitions: Keys to Unlocking the Value of Synergy," MIT, 1999.

[21] T. TETENBAUM, "Improve the Chance for Expecte(d Integration and Synergies," *ORGANIZATIONAL DYNAMICS*, Autumn 1999.

[22] J. Haleblian, "Taking Stock of What We Know About Mergers and Acquisitions: A Review and Research Agenda," *Journal of Management,* vol. 35, no. 3, pp. 469-502, 2009.

[23] F. Heylighen, "Complexity and Self-organization," in *Encyclopedia of Library and Information Sciences*, M. J. B. a. M. N. Maack, Ed., Taylor & Francis, 2008.

[24] R. Sandhu and P. Samarati, "Access Control: Principles and Practice," *IEEE Communications,* pp. 40-48, September 1994.

[25] W. Ware, "Security Controls for Computer Systems: Report of Defence Science Board Task Force on Computer Security," Rand Report R609-1, 1970.

[26] W. Diffe and M. Hellman, "New directions in Cryptography," *IEEE Transactions in Information Theory,* vol. 22, no. 6, pp. 644-654, 1976.

[27] M. Bishop, Computer Security – Art and Science, Addison-Wesley, 2002.

[28] P. P. GRIFFITHS and B. W. WADE, "An Authorization Mechanism for a Relational Database System," *ACM Transactions on Database Systems,* vol. Vol. 1, no. 3, pp. 242-255, eptember 1976.

[29] G. J. POPEK and C. S. KLINE, "Encryption and Secure Computer Networks," *Computing Surveys,* vol. 11, no. 4, pp. 331-356, December 1979.

[30] S. T. Walker, "Network security overview," *Proceedings of the 1985 IEEE Symposium on Security and Privacy,* pp. 22-24, 1985.

[31] B. Lampson, "Protection," in *Princeton Symposium of Information Science and Systems*, 1971.

[32] G. Graham and P. Denning, "Protection – Principles and Practice," in *AFIPS Spring Joint Computer Conference*, 1972.

[33] M. Harrison, W. Ruzzo and J. Ullman, "Protection in Operating Systems," *Communications of the ACM,* vol. 19, no. 8, pp. 461-471, August 1976.

[34] D. Bell and L. LaPadula, "Secure Computer Systems: Mathematical Foundations," MITRE Corporation, 1973.

[35] K. Biba, "Integrity Considerations for Secure Computer Systems," MITRE Corporation, Apr 1977.

[36] L. Snyde, "Formal Models of Capability-Based Protection Systems," *IEEE Transactions on Computers,* March 1981.

[37] R. Sandhu, "Rationale for the RBAC96 family of access control models," in *Proceedings of the 1st ACM Workshop on Role-Based Access Control,* 1997.

[38] G. S. Benson, I. F. Akyildiz and W. F. Appelbe, "A formal protection model of security in centralized, parallel, and distributed systems," *ACM Transactions on Computer Systems (TOCS)* , vol. 8, no. 3, August 1990 .

[39] R. . S. Sandhu, "The Typed Access Matrix Model," in *Proceedings of IEEE Symposium on Security and Privacy,* Oakland, 1992.

[40] P. E. Ammann and R. S. Sandhu, "The Extended Schematic Protection Model," *Journal of Computer Security,* pp. 335-383, 1992.

[41] D. D. Denning, "A lattice model of secure information flow," *Communications of the ACM,* vol. 19, no. 5, pp. 236-243, 1976.

[42] L. Liu, "On Secure Flow Analysis in Computer Systems," in *IEEE Symposium on Research in Security and Privacy,* 1980.

[43] J. McLean, "The specification and modeling of computer security," *IEEE EXplore*, vol. 23, no. 1, pp. 9-16, 1990.

[44] M. Bykova, "What Should a Good Security Model Be?," Purdue University, 2004.

[45] C. McCollum, J. Messing and et. al., "Beyond the Pale of MAC and DAC – Defining New Forms of Access Control," in *IEEE Computer Society Symposium on Research in Security and Privacy.*, 1990.

[46] D. Ferraiolo, J. Cugini and R. Kuhn, "Role-based access control (RBAC): Features and motivations," in *Proceedings of 11th Annual Computer Security Application Conference*, 1995.

[47] R. S. Sandhu, E. J. Coyne and et. al., "Role-based Access Control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38-47, February 1996.

[48] D. Ferraiolo, R. Kuhn and R. Chandramouli, Role-based Access control, Information Systems Audit and Control Association, 2004.

[49] E. Bertino, P. Bonatti and E. Ferrari, "TRBAC: A Temporal Role Based Access Control Model," in *ACM Workshop on Role-based Access Control*, 2000.

[50] J. Joshi, E. Bertino and et. al., "Generalized Temporal Role Based Access Control Model (GTRBAC) (Part I) Specification and Modeling," Purdue University, 2001.

[51] P. Chillakanti, "Role-based information security: change management issues," in *Proceedings of the 2004 international symposium on Information and communication technologies*, 2004.

[52] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized Trust Management," in *IEEE Symposium on Security and Privacy*, 1996.

[53] W. Winsborough, K. Seamons and V. Jones, "Automated Trust Negotiation," in *DARPA Information*

Survivability Conference and Exposition (DISCEX 2000), 2000.

[54] W. Winsborough and N. Li, "Towards Practical Automated Trust Negotiation," in *IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2002)*, 2002.

[55] N. Li, W. Winsborough and J. Mitchell, "Distributed Credential Chain Discovery in Trust Management," in *ACM Conference on Computer and Communications Security*, 2001.

[56] Y. Ting and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in *Proceedings. 2003 Symposium on Security and Privacy*, 2003.

[57] T. Ryutov, L. Zhou and et. al., "Adaptive trust negotiation and access control," in *Proceedings of the tenth ACM symposium on Access control models and technologies* , 2005.

[58] R. Khare and A. Rifkin, "Weaving a Web of Trust," *World Wide Web Journal, special issue on security*, vol. 2, no. 3, pp. 77-112, 1997.

[59] B. Blakley, "The Emperor's Old Armor," in *ACM New Security Paradigms Workshop (NSPW)*, 1996.

[60] D. Smetters and R. Grinter, "Moving from the Design of Usable Security Technologies to the Design of Useful Secure Applications," in *ACM New Security Paradigms Workshop (NSPW)*, 2002.

[61] D. Boneh and M. Franklin, "Identity-base Encryption from the Weil Pairing ,," in *CRYPTO 2001*, 2001.

[62] R. Nelson, "Unhelpfulness as a Security Policy or It's About Time," in *ACM New Security Paradigms Workshop (NSPW)*, 1995.

[63] H. Lipson and D. Fisher, "Survivability — A New Technical and Business Perspective on Security," in *ACM New Security Paradigms Workshop (NSPW), pp. 33–39*, 1999.

[64] D. Weirich and M. Sasse, "Pretty Good Persuasion: A First Step towards Effective Password Security in the

Real World," in *ACM New Security Paradigms Workshop (NSPW)*, 2001.

[65] A. Somayaji and S. Hofmeyr, "Principles of a Computer Immune System," in *ACM New Security Paradigms Workshop (NSPW)*, 1997.

[66] J. Williams, "Just Sick About Security," in *ACM New Security Paradigms Workshop (NSPW)*, 1996.

[67] D. Povey, "Optimistic Security: A New Access Control Paradigm," in *ACM New Security Paradigms Workshop (NSPW)*, 1999.

[68] D. Welch, N. Buchheit and A. Ruocco, "Strike Back: Offensive Actions in Information Warfare," in *ACM New Security Paradigms Workshop (NSPW)*, 199.

[69] L. Spitzner, "http://spitzner.net/honeypots.html," [Online]. Available: http://spitzner.net/.

[70] R. Nelson, "What is a Secret – and – What does it have to do with Computer Security?," in *ACM New Security Paradigms Workshop (NSPW)*, 1994.

[71] G. McGraw, Software Security: Building Security In, Addison-Wesley, 2006.

[72] G. McGraw, "From the ground up: the DIMACS software security workshop," *Security & Privacy*, vol. 1, no. 2, pp. 59-66, 2003.

[73] H. Munawar and et.al., "Organizing security patterns," *Software*, vol. 24, no. 4, pp. 52-60, 2007.

[74] T. Sander and C. F. Tschudin, "On the Cryptographic Protection of Mobile Code," in *Proceedings of the Workshop on Mobile Agents and Security*, 1997.

[75] H. Gao and et. al., "SEcurity Issues in Online Social Networks," *IEEE Internet Computing*, pp. 56-63, July 2011.

[76] C. Rose, "The Security Implications of Ubiquitous Social Media," *International Joournal of Management and Information Systems,* vol. 15, no. 1, pp. 35-40, First Quarter 2011.

[77] S.-W. Seong, "PRPL: A Decentralized Social Networking Infrastructure," Stanford university, 2010.

[78] P. Gundecha and et. al., "Exploiting Vulnerability to Secure User Privacy on a Social Networking Site," in *KDD'11*, San Diego, 2011.

[79] M. Backes and et.al., "A Security API for Distributed Social Networks".

[80] E. Aïmeur and et.al., "Towards a Privacy-enhanced Social Networking Site," *IEEE Computer Society*, pp. 172-179, 2010.

[81] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," US Department of Commerce, 2011.

[82] B. Hay and et.al., "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing," in *Proceedings of the 44th Hawaii International Conference on System Sciences*, Hawaii, 2011.

[83] W. Janse and T. Grance , "Guidelines on Security and Privacy in Public Cloud Computing," Department of Commerce, 2011.

[84] M. Almorsy and et.al., "Collaboration-Based Cloud Computing Security Management Framework," in *IEEE 4th International Conference on Cloud Computing*, 2011.

[85] D. Jamil and et.al., "CLOUD COMPUTING SECURITY," *International Journal of Engineering Science and Technology (IJEST),* vol. 3, no. 4, pp. 3478-3483, April 2011.

[86] . Z. Dimitrios and L. Dimitrios, "Addressing cloud computing security issues," *Future Generation Computer Systems,* pp. 583-592, 2010.

[87] S. O. Kuyoro and et. al., "Cloud Computing Security Issues and Challenges," *International Journal of*

Computer Networks (IJCN),, vol. 3, no. 5, pp. 247-255, 2011.

[88] P. W. Mattessich and B. R. Monsey, "Collaboration: What Makes It Work. A Review of Research Literature on Factors Influencing Successful Collaboration," in *Collaboration Handbook: Creating, Sustaining, and Enjoying the Journey*, St. Paul, MN: Amherst H. Wilder Foundation, 1994.

[89] P. Johnson, "Collaboration in the Small vs. Collaboration in the Large," in *Proceedings of the 1994 CSCWWorkshop on Software Architectures for Cooperative Systems*, Chapel Hill, Virginia, 1994.

[90] G. Wiederhold, M. Bilello and et.al., "Protecting Collaboration," in *Proceedings of the NISSC'96 National Information Systems Security Conference*, 1996.

[91] J. William, M. Srilekha and M. Thompson, "Authorization and attribute certificates for widely distributed access control," in *Proceedings Seventh IEEE International Workshop on Enabling Technologies: Infrastucture for Collaborative Enterprises (WET ICE '98)*, 1998.

[92] R. Caralli and L. Young, "Focus on Resiliency: A Process Improvement Approach to Security," in *CSI 33rdAnnual Security Conference and Exhibition*, 2006.

[93] L. Pearlman, V. Welch and et. al., "A community authorization service for group collaboration," 2002.

[94] D. Olmedilla and O. Rana, "Security and trust issues in semantic grids," 2005.

[95] D. Artz and Y. Gil, "A survey of trust in computer science and the semantic web," *Web Semantics: Science, Services and Agents on the World Wide Web,* vol. 5, no. 2, pp. 58-71, 2007.

[96] T. Berners-Lee and J. Hendler, "The semantic web," *Scientific American,* vol. 284, no. 5, pp. 28-37, 201.

[97] F. Guti´errez Vela, "An architecture for access control management in collaborative enterprise systems based on organization models," in *Science of Computer Programming* , vol. 66, Elsevier, 2007, pp. 44-59.

[98] C. A. Ellis, S. J. Gibbs and et. al., "Groupware:Some Issues and Experiences," *Communications of the ACM*, vol. 34, no. 1, pp. 38-58, 1991.

[99] W. Tolone and et. al., "Access Control in Collaborative Systems," *ACM Computing Surveys*, vol. 37, March 2005.

[100] P. Nasirifard, "Context-Aware Access Control for Collaborative Working Environments Based on Semantic Social Networks," National University of Ireland, Galway, 2007.

[101] "First World Congress of Transdisciplinarity," in *First World Congress of Transdisciplinarity*, Convento da Arrábida, Portugal, 1994.

[102] A. Imine, "A Flexible Access Control Model for Distributed Collaborative Editors," in *SDM 2009, LNCS 5776*, W. J. a. M. Petkovi´c, Ed., 2009, p. 89–106.

[103] J. Arnedo-Moreno, "Collaborative group membership and access control for JXTA," in *Communication Systems Software and Middleware Workshop. 3rd International Conference on Communication*, 2008.

[104] CIO Council, "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation, Version 1.0.," 2009.

[105] O. Moonian, "HCRBAC – An Access Control System for Collaborative Context-Aware HealthCare Services in Mauritius," *Journal of Health Informatics in Developing Countries*, vol. 2, no. 2, 2008.

[106] A. Gouglidis, "domRBAC: An access control model for modern collaborative systems," *Computers & Security*, vol. 31, no. 4, 2012.

[107] W. Stallings, "Standards for Information Security Management," *The Internet Protocol Journal*, vol. 10, no. 4, December 2007.

[108] JISC, "Identity & Access Management using Social Networking Technologies – Final Report," July 2011. [Online]. Available: http://www.rcs.manchester.ac.uk/research/FoafSslShib.

[109] "http://www.businessdictionary.com/definition/self-organization.html," [Online]. Available: http://www.businessdictionary.com.

[110] C. Gerhenson and et. al., "When can we call a system self-organizing?," in *7th European Conference on Advances in Artificial Life (ECAL)*, Dortmund, Germany, 2003.

[111] N. Fernandes and et. al., "A Self-Organized Mechanism for Thwarting Malicious Access in Ad Hoc Networks," in *INFOCOM' 10 Proceedings of the 29th conference on Information Systems*, 2010.

[112] R. Savola, "Node Level Security Management and Authentication in Mobile Ad Hoc Networks," in *Tenth International Conference on Mobile Data Management: Systems, Services and Middleware*, Taipei, Taiwan, 2009.

[113] G. Castelli and et. al., "A Self-Organized Multiagent Approach for Distributed Management of Contextual Data, Mobile Wireless Middleware, Operating Systems, and Applications," in *Third International Conference, Mobilware 2010*, Chicago, IL, USA, 2010.

[114] F. Dressler, "A Study of Self-Organization Mechanisms in Ad Hoc and Sensor Networks," in *Computer Communications*, Elsevier, 2008.

[115] M. Mamei and et. al., "Case Studies of Self-Organization in Computer Science," *Journal of systems Architecture*, vol. 52, no. 8-9, pp. 443-460, 2006.

[116] M. Bhakti and et. al., "Nature-Inspired Self Organizing Service Oriented Architecture: A Proposal," in *International Conference on Information Technology in Asia (CITA 2009)*, Kuching, Sarawak, Malaysia, 2009.

[117] C. Gershenson, "A General Methodology for Designing Self-Organizing Systems, Technical Report 2005-05," ECCO, 2006.

[118] A. Forestiero and et. al., "Self-Chord: a Bio-Inspired P2P Framework for Self-Organizing Distributed Systems," *IEEE/ACM Transactions on Networking*, vol. 18, no. 5, pp. 1651-1664, October 2010.

[119] W. R. Ashby, "Principles of the self-organizing systems," in *Principles of Self-Organization:Transactions of the University of Illinois Symposium*, 1962.

[120] "http://www.iso27001security.com/html/iso27000.html," [Online].

[121] "http://csrc.nist.gov/," [Online].

[122] "http://www.nist.gov/itl/upload/draft_outline_preliminary_framework_standards.pdf," [Online].

[123] P. Chillakanti and et. al., "Evolution of Security Paradigms, Frameworks, and Models," in *SDPS 2011: Technology Innovation through Transformative Synthesis*, Jeju Island, South Korea, 2011.

[124] "http://dictionary.reference.com/browse/methodology," [Online].

[125] "http://www.businessdictionary.com/definition/methodology.html," [Online].

[126] "http://dictionary.reference.com/browse/trust," [Online].

[127] "http://www.businessdictionary.com/definition/method.html," [Online].

[128] "http://dictionary.reference.com/browse/method," [Online].

[129] "http://dictionary.cambridge.org/dictionary/british/method," [Online].

[130] "http://dictionary.cambridge.org/dictionary/british/technique," [Online].

[131] "http://dictionary.reference.com/browse/technique," [Online].

[132] "http://www.businessdictionary.com/definition/technique.html," [Online].

[133] "http://www.businessdictionary.com/definition/research-methodology.html," [Online].

[134] S. Rajasekar, P. Philominathan and V. Chinnathambi, "RESEARCH METHODOLOGY," arxiv.org Cornell University, 2006.

[135] W. Goddard and S. Melville, "Introduction," in *Research Methodology: An Introduction*, Lansdowne, Juta & Co Ltd., 2007.

[136] C. R. Kothari, "Research Methodology: An Introduction," in *Research Methodology : Methods and Techniques*, New Age International Publishers, 2012, pp. 1-23.

[137] School of Management, "Introduction to Research and Research Methods".

[138] G. Degu and T. Yigzaw, "Research Methodology," University of Gondar, 2006.

[139] J. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Method Approaches, California: Sage Publications, 2003.

[140] M. BORREGO, E. Douglas and C. AMELINK, "Quantitative, Qualitative, and Mixed Research Methods in Engineering Education," *Journalo f EngineeringE ducation*, vol. 98, no. 1, pp. 53-66, January 2009.

[141] R. J. Clarke, "Research Models and Methodologies," Wollongong, Australia, 2005.

[142] L. Christensen, R. B. Johnson and L. Turner, "Chapter 13: Qualitative and Mixed Methods Research," in *Research Methods, Design, and Analysis*, Pearson, 2011.

[143] University of Kansas Libraries, "http://www.lib.ku.edu/splat/coursepages/general/FormulatingaResearchQuestion.pdf," [Online].

[144] R. Marion , "The Whole Art of Deduction: Research Skills for new Scientists," 2004.

[145] E. E. Lipowski, "Developing Great Research Questions," *American Joutnal of Health-System Pharmacists*, vol. 65, pp. 16667-1670, September 2008.

[146] C. Moser and G. Kalton, Survey methods in social investigation, 2nd ed., Dartmouth: Aldershot, 1993.

[147] D. Ferraiolo, D. Kuhn and et. al., "Role-Based Access Control (RBAC)," in *15th National Computer Security Conference*, 1992.

[148] D. Ferraiolo, R. Sandhu and et. al., "Proposed NIST Standard for Role-Based Access Control," *ACM Transactions on Information and System Security,* vol. 4, no. 3, pp. 224-274, August 2001.

[149] S. Oh and R. Sandhu, "A model for role administration using organization structure," in *Proceedings of the 7th ACM symposium on Access control models and technologies*, Monterey, CA , 2002.

[150] E. Yuan and J. Tong, "Attributed Based Access Control (ABAC) for Web Services," in *Proceedings of theIEEE International Conference on Web Services, ICWS '05*, Washington, DC, 2005.

[151] J. Joshi and Y. Zhang, "ARBAC07: a role-based administration model for RBAC with hybrid hierarchy," in *IRI'07: Proceedings of the IEEE International Conference on Information Reuse and Integration*, 2007.

[152] P. Chen, "Toward a Unified View of Data," *ACM Transactions on Database Systems,* vol. 1, pp. 9-36, 1976.

[153] I. A. Tondel, M. G. Jaatun and et. al., "Security Requirements for the Rest of Us: A Survey," *IEEE Software,* pp. 20 -27, January 2008.

[154] D. G. Firesmith, "Engineering Security Requirements," *Journal of Object Technology*, vol. 2, no. 1, pp. 53-68, 2003.

[155] C. B. Haley, R. Laney and et. al., "Security Requirements Engineering: A Framework for Representation and

Analysis," *IEEE Transaction on Software Engineering*, vol. 34, no. 1, pp. 133-153, 2008.

[156] M. Bishop, "What is Computer Security," *IEEE Security and Privacy*, pp. 67-69, January 2003.

[157] "http://oxforddictionaries.com/us/definition/american_english/trust," [Online].

[158] "http://dictionary.reference.com/browse/trust," [Online].

[159] V. Cahill and E. Gray, "Using trust for secure collaboration in uncertain environments," *Pervasive Computing*, vol. 2, no. 3, pp. 52-61, 2003.

[160] C. Castelfranchi and R. Falcone, "Principles of trust for MAS: Cognitive anatomy, social importance, and quantification," in *Proceeding of ICMAS'98*, 1998.

[161] T. Grandison and M. Sloman, "Specifying and analysing trust for internet applications," in *Proceedings of the IFIP Conference on Towards The Knowledge Society: E-Commerce, E-Business, E-Government*, 2002.

[162] T. Grandison and M. Sloman, "A survey of trust in internet applications," *Communications Surveys & Tutorials, IEEE* , vol. 3, no. 4, pp. 2-16, 20000.

[163] J. Myhill, "The abstract theory of self-reproduction," *Views on general systems theory*, pp. 106-118, 1964.

[164] D. M. MIHAJLO, "FOUNDATIONS FOR A General Systems Theory," in *Proceedings of the Second Systems Symposium at Case Institute of Technology*, New York, 1964.

[165] C. Gershenson, "Design and Control of Self-organizing Systems," VRIJE Universiteit Brussel, 2007.

[166] S. N. Salthe, "Self-organization of/in hierarchically structured systems," *Systems Research*, vol. 6, no. 3, pp. 199-208, 1989.

[167] "http://wikepedia.org/sel-organizaation," [Online].

[168] T. Misteli, "The concept of self-organization in cellular architecture," *Journal of Cell Biology,* vol. 155, no. 2, pp. 181-186, 2001.

[169] F. Heylighen, "The science of self-organization and adaptivity," *The Encyclopedia of Life Support Systems,* vol. 5, no. 3, pp. 253-280, 2001.

[170] P. Watzlawick and J. H. Weakland, Change: Principles of problem formation and problem resolution, WW Norton, 1974.

[171] M. Deutsch and R. M. Krauss, Theories in social psychology, Basic Books, 1965.

[172] M. H. Kavanagh and N. M. Ashkanasy, "The impact of leadership and change management strategy on organizational culture and individual acceptance of change during a merger," *British Journal of Management,* vol. 17, no. S1, pp. S81--S103, 2006.

[173] J. P. Kotter, "Leading change: Why transformation efforts fail," *Harvard Business Review,* vol. 73, no. 2, pp. 59-67, 1995.

[174] W. Bridges and S. Mitchell, "Leading transition: A new model for change," *Leader to Leader,* vol. 16, no. 3, pp. 30-36, 2000.

[175] S. L. Pfleeger, "Understanding and improving technology transfer in software engineering," *Journal of Systems and Software,* vol. 47, no. 2, pp. 111-124, 1999.

[176] R. Seel , "http://www. heacademy. ac. uk/assets/York/documents/ourwork/changeacademy/2007/CA018D_Seel_NatureOfOrganisationalChange," 2007. [Online].

[177] T. Creasey, "Defining change management," Prosci and the Change Management Learning Center, 2007.

[178] SG3, "Quality Management Systems - Process Validation Guidance," GHTF Study Group 3, 2004.

[179] IEEE, "IEEE Guide--Adoption of the Project Management Institute (PMI®) Standard: A Guide to the Project Management Body of Knowledge (PMBOK® Guide)," IEEE, 2011.

Appendix A: Log Entry from Experiential Project

Example: This is a case entered by an internal team and its focus is on access control management. The text in the box is from the log and not the wording of this research. The acquiring company is denoted by “XYZ”, and other companies involved in the acquisition onboarding are denoted by similar symbols to protect the confidentiality of the companies.

Partners Team	***Preventing Access for Competitors at Registration***
Business Function	***Channel Partner Support***
	Case Summary *The Channel Partner Onboarding team, Channel Partner Competitive Office, Channel Partner Data Strategy and Governance team, Brand Protection team and Corporate Learning Office (CLO) collaborated to investigate two problem areas. First, our company XYZ allows direct competitors and their subsidiaries to register as channel partners. This allows registered competitors unrestricted access to partner level, XYZ confidential Intellectual Property including pricing strategies and discount promotions, marketing materials, and software downloads. Secondly, XYZ allows individuals who work for direct competitors to create and use XYZ IDs on XYZ.com. With over 1000 overt ABC, DEF, and GHI employees identified with active ID's, competitors have used the XYZ.com site to gather competitive intelligence. Other cross-functional stakeholders, including Legal, Export Control Team, Channels Data Enablement, Strategic Marketing Organization, and Services Entitlement were engaged to confirm the issues and uncover additional improvement actions.* *The investigation led to several process-related recommendations around decision-making, ownership, documentation, communications, and governance to drive consistency in the prevention of direct competitors gaining access to XYZ intellectual property, marketing, and strategy*

	roadmaps. ***Criticality and Risk*** *Allowing named direct competitors and individuals who work for direct competitors to register as channel partners and XYZ guest user results in exposure to IP loss, reduced competitive advantage, and unethical use of insider information to gain market share.* ***Lessons Learned*** *1. The lack of screening at registration allows competitor employees to register at XYZ.com and direct competitors to register as channel partners resulting in overt competitive intelligence gathering and theft of XYZ's intellectual property.* *2. The lack of centralized user access content management for XYZ.com results in intellectual property leakage, increasing the risk for competitive advantage abuse.* *3. Lack of standardization across published content results in an unknown amount of improperly entitled content, increasing the risk for content to be leveraged for competitive advantage* *4. Without consistent governance, IP loss/abuse is not tracked, measured or monitored within or across all tiered levels at XYZ.com* *Recommendation: Establish a governance review team for XYZ.com content management. Determine feasibility for identification of content based on category and level access across XYZ.com and establish a process to review / pull exposed information.*

Appendix B: Collaboration Security Survey – Pilot

In Mergers and Acquisitions, when a company acquires another company, there is inter-enterprise collaboration. The purpose of this survey is to gain insights into the following in this context.

1. Understand and assess the process of on boarding acquired companies

2. Understand and assess the access control management in inter-enterprise collaboration

* Required

1. Name *

State your name

2. Can I follow up with you? If so give your email address and contact number

3. Your organizational role *

(Which department you belong to? Mark only one oval.)

- ○ HR
- ○ IT
- ○ Sales and Marketing
- ○ Channels and Partner Support
- ○ Business Functional Unit
- ○ Learning and Development
- ○ Other

4. What is your role in acquisition integration? *

What specific role you play in on boarding acquisitions (select one or more options). Check all that apply.

- ■ Team Leader
- ■ Integration Manager
- ■ HR Integration
- ■ IT Integration
- ■ Sales and Marketing Integration
- ■ Channel Partner Integration
- ■ Business Unit Integration

5. At what stage of on boarding is your first involvement? *

Mark only one oval.

- ○ Immediately after deal close and acquisition integration begins
- ○ Acquisition integration team requests my participation during the on boarding process
- ○ Just before acquisition integration is complete and signed off by stakeholders

6. My roles and responsibilities are clearly defined in on boarding *

Mark only one oval.

- ○ completely agree
- ○ somewhat agree

- ○ somewhat disagree
- ○ completely disagree

7. I have a clear understanding of my immediate collaboration team member with who I interact with on an almost daily basis *

Mark only one oval.

- ○ completely agree
- ○ somewhat agree
- ○ somewhat disagree
- ○ completely disagree

8. Information sharing and access control management in on boarding explained to the team clearly *

Was it clear to you about what you can share and how you can share when you participate in onboarding?

Mark only one oval.

- ■ completely agree
- ■ somewhat agree
- ■ somewhat disagree
- ■ completely disagree

9. What was the method of sharing documents? *

Check all that apply.

- email
- internal collaboration workspace
- Google Drive
- Dropbox
- internal collaboration workspace
- Other:

10. Did you set up access control management for granting access to the documents that you shared? *

    Mark only one oval.

    - yes
    - no

11. Did you have access to all on boarding related documents in the collaboration work space or central repository? *

    Mark only one oval.

    - yes
    - no

12. How would someone request access to your documents in the shared workspace? *

    Check all that apply.

    - everyone has access to all documents in the work space

- they send me a request by email to grant them access to my document in the work space
- the collaboration system has mechanisms to request access

13. How do you grant access to documents? *

Check all that apply.

- Everyone has access to all documents in the work space
- I grant access using the mechanisms of the collaboration work space
- I email them the documents that they requested
- I seek approval of my on boarding team lead

14. Did you access documents in the collaboration work space which were not directly related to your on boarding role? *

Check all that apply.

- sometimes opened documents accidentally
- never accessed unrelated documents
- sometimes opened documents to find out if I needed them
- I opened other documents to gain broader understanding

15. Did you have clarity about process life cycle of on boarding acquisitions? *

Mark only one oval.

- I had complete clarity of process
- I had about 75% clarity of the process

- I had less than 50% clarity of process
- I think the process was not clear at all

16. I know when my role in the on boarding begins and ends *

    Mark only one oval.

    ○ completely agree
    ○ somewhat agree
    ○ somewhat disagree
    ○ completely disagree

17. For each process step in on boarding acquisition, the roles and responsibilities were clearly defined *

    Mark only one oval.

    ○ completely agree
    ○ somewhat agree
    ○ somewhat disagree
    ○ completely disagree

18. The inter-enterprise collaboration process is defined completely and accurately *

    Mark only one oval.

    ○ Completely agree
    ○ Somewhat agree
    ○ Somewhat disagree

- ○ Completely disagree

19. The milestones and measurement of process quality were satisfactory *

Mark only one oval.

- ○ completely agree
- ○ somewhat agree
- ○ somewhat disagree
- ○ completely disagree

20. Risk Management strategies were well defined to manage project timelines and personnel changes *

Mark only one oval.

- ○ completely agree
- ○ somewhat agree
- ○ somewhat disagree
- ○ completely disagree

21. When a person's role ended during collaboration their access to collaboration space was terminated? *

Mark only one oval.

- ○ access terminated immediately and team got notified
- ○ there was a time lag in terminating access

- ○ people had access to collaboration work space even after the on boarding was completed
- ○ the information about whose role ended was not available

22. The on boarding project closure was defined clearly *

Mark only one oval.

- ○ completely agree
- ○ somewhat agree
- ○ somewhat disagree
- ○ completely disagree

23. I had access to collaboration work space even after the project officially closed *

Mark only one oval.

- ○ My access still existed at least one month after closure
- ○ My access terminated on the day of closure
- ○ I had access for up to a week after closure
- ○ Access was never terminated

24. Anyone can put documents in the collaboration work space *

Mark only one oval.

- ○ yes any team member can put documents in the workspace
- ○ only team leader can put documents in the work space

25. The assignment of roles and access control is clearly defined *

Mark only one oval.

- ○ completely agree
- ○ somewhat agree
- ○ somewhat disagree
- ○ completely disagree

26. Do you use any trust management schemes to grant access to documents in work space? *

Mark only one oval.

- ○ No, all members have access to documents
- ○ Yes, we use trust management schemes to determine access dynamically
- ○ access control is determined by statically defined policies
- ○ if someone does not have access but I trust them I share the documents

27. I get notifications when new documents are put in the collaboration workspace *

Mark only one oval.

- ○ always because the system notifies to everyone
- ○ sometimes because the individual who put the document can specify the people who should be notified
- ○ the system does not have automatic notification mechanisms

28. In your opinion how effectively collaboration security in terms of access control is managed in on boarding acquisitions? *

Please write your thoughts based on your experience

29. What process improvement suggestions you may have for onboarding acquisitions *

Appendix C: Collaboration Security Survey – Final

Thank you for your participation in this survey which is part of my PhD dissertation. All of your information will remain anonymous and the survey results will be discussed in my dissertation in aggregate form. If you have any questions, please contact me at pratap@lensoo.com.

In Mergers and Acquisitions, when a company acquires another company, there is inter-enterprise collaboration. The purpose of this survey is to gain insights into the following in this context.

1. Understand and Assess the process of on boarding acquired companies
2. Understand and Assess the access control management in inter-enterprise collaboration

* Required

1. Name

State your name

2. Your organizational role *

Which department do you belong to? Mark only one oval.

- ○ HR
- ○ IT
- ○ Sales and Marketing
- ○ Channels and Partner Support

- ○ Business Functional Unit
- ○ Learning and Development
- ○ Other

3. What is your role in acquisition integration? *

What specific role you play in onboarding acquisitions (select one or more options)? Check all that apply.

- ■ Team Leader
- ■ Integration Manager
- ■ HR Integration
- ■ IT Integration
- ■ Sales and Marketing Integration
- ■ Channel Partner Integration
- ■ Business Unit Integration

4. At what stage of on boarding is your first involvement? *

Mark only one oval.

- ○ Immediately after deal close and acquisition integration begins
- ○ Acquisition integration team requests my participation during the on boarding process
- ○ Just before acquisition integration is complete and signed off by stakeholders

5. My roles and responsibilities are clearly defined in onboarding *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

6. I have a clear understanding of my immediate collaboration team members *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

7. Information sharing and access control management in on boarding explained to the team clearly *

Was it clear to you about what you can share and how you can share when you participate in onboarding? Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

8. What was the method of sharing documents? *

Check all that apply.

- email
- internal collaboration workspace
- Google Drive
- Dropbox
- internal collaboration workspace
- Other:

9. Did you set up access control management for granting access to the documents that you shared? *

Mark only one oval.

- ○ yes
- ○ no

10. Access control to the documents that I shared is set up by *

Check all that apply.

- myself - I determine who gets access
- IT admin -- I give them the list of people who can access
- my team leader -- I give him the list of potential people who can access
- everyone gets access to all documents during the course of onboarding

11. Did you have access to all onboarding related documents in the collaboration work space or central repository? *

Mark only one oval.

- ○ yes
- ○ no

12. How would someone request access to your documents in the shared work space?*

Check all that apply.

- ■ everyone has access to all documents in the work space
- ■ they send me a request by email to grant them access to my document in the work space
- ■ the collaboration system has features to request/grant access

13. How do you grant access to documents? *

Check all that apply.

- ■ everyone has access to all documents in the work space
- ■ I grant access using the features of the collaboration system to grant/request access
- ■ I email them the documents that they requested
- ■ I seek approval of my onboarding team lead

14. Did you access documents in the collaboration work space which were not directly related to your onboarding role? *

Check all that apply.

- sometimes opened documents accidentally
- never accessed unrelated documents
- sometimes opened documents to find out if I needed them
- I opened other documents to gain broader understanding

15. Did you have clarity about process life cycle of onboarding acquisitions? *

Mark only one oval.

- ○ I had complete clarity of process
- ○ I had about 75% clarity of the process
- ○ I had less than 50% clarity of process
- ○ I think the process was not clear at all

16. I know when my role in the onboarding begins and ends *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

17. For each process step in onboarding acquisition, the roles and responsibilities were clearly defined *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

18. The inter-enterprise collaboration process is defined completely and accurately *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

19. The milestones for onboarding process are defined satisfactorily *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

20. The metrics for measurement of onboarding process progress are defined satisfactorily *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

21. Risk Management strategies are well defined to manage project timelines *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

22. Risk Management strategies are well defined to manage personnel changes during onboarding process *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree
- ○ strongly disagree

23. When a person's role ended during collaboration their access to collaboration space was terminated? *

Mark only one oval.

- ○ access terminated immediately and team got notified
- ○ there was a time lag in terminating access
- ○ people had access to collaboration work space even after the onboarding was completed
- ○ the information about whose role ended was not available

24. I had access to collaboration space even after the onboarding project officially closed *

Mark only one oval.

- ○ my access existed for at least one month after close of project
- ○ my access terminated on the day of onboarding project closure
- ○ I had access for up to a week after onboarding project closure
- ○ access was never terminated

25. The onboarding project closure is defined clearly *

Mark only one oval.

- ○ strongly agree
- ○ mostly agree
- ○ somewhat disagree

○ strongly disagree

26. Anyone can put documents in the collaboration work space *

Mark only one oval.

○ yes any team member can put documents in the workspace

○ only team leader can put documents in the work space

27. The assignment of roles and access control is clearly defined for onboarding process lifecycle *

Mark only one oval.

○ strongly agree

○ mostly agree

○ somewhat disagree

○ strongly disagree

28. Do you use any trust management techniques to grant access to documents in work space?*

Mark only one oval.

○ No, all members have access to documents

○ Yes, we use trust management techniques to determine access dynamically

○ access control is determined by statically defined policies

○ if someone does not have access but I trust them I share the documents

29. I get notifications when new documents are put in the collaboration workspace *

Mark only one oval.

- ○ always because the system notifies everyone
- ○ sometimes because the individual who put the document can specify the people who should be notified
- ○ the system does not have automatic notification mechanisms

30. In your opinion how effectively collaboration security (in terms of access control) is managed in onboarding acquisitions?*

Please write your thoughts based on your experience

31. What process improvement suggestions you may have for onboarding acquisitions?

32. Anything else you would like to share in terms of onboarding process and collaboration security?

33. May I follow up with you? If so, please give your contact number and email.

Appendix D: Survey – Final Summary Responses

Name

Removed for confidentiality

Your organizational role

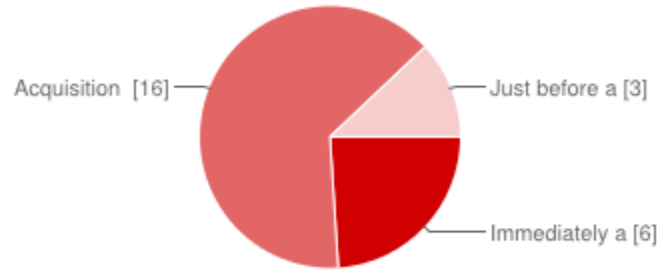
HR	2	8%
IT	5	20%
Sales and Marketing	4	16%
Channels and Partner Support	1	4%
Business Functional Unit	7	28%
Learning and Development	3	12%
Other	3	12%

What is your role in acquisition integration?

Team Leader	5	17%
Integration Manager	0	0%

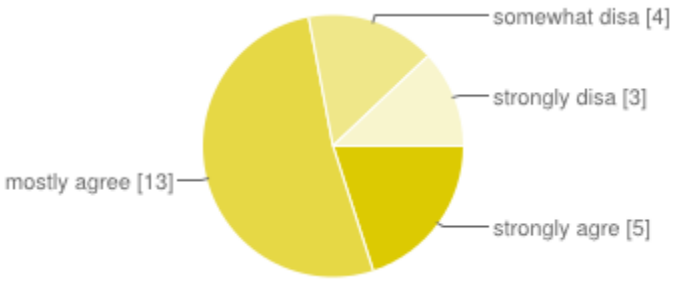
HR Integration	3	10%
IT Integration	6	20%
Sales and Marketing Integration	5	17%
Channel Partner Integration	5	17%
Business Unit Integration	6	20%

At what stage of on boarding is your first involvement?



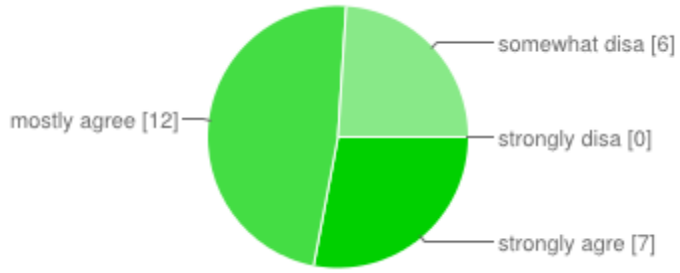
Immediately after deal close and acquisition integration begins	6	24%
Acquisition integration team requests my participation during the on boarding process	16	64%
Just before acquisition integration is complete and signed off by stakeholders	3	12%

My roles and responsibilities are clearly defined in onboarding



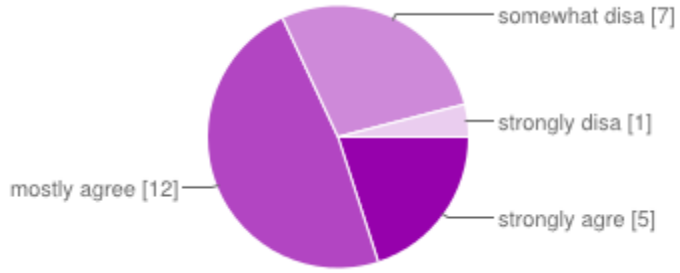
strongly agree	5	20%
mostly agree	13	52%
somewhat disagree	4	16%
strongly disagree	3	12%

I have a clear understanding of my immediate collaboration team members



strongly agree	7	28%
mostly agree	12	48%
somewhat disagree	6	24%
strongly disagree	0	0%

Information sharing and access control management in on boarding explained to the team clearly



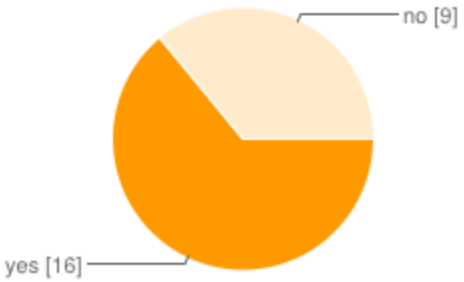
strongly agree	5	20%
mostly agree	12	48%
somewhat disagree	7	28%

strongly disagree	1	4%

What was the method of sharing documents?

email	16	18%
internal collaboration workspace	32	36%
Google Drive	2	2%
Dropbox	4	5%
internal collaboration workspace	32	36%
Other	2	2%

Did you set up access control management for granting access to the documents that you shared?

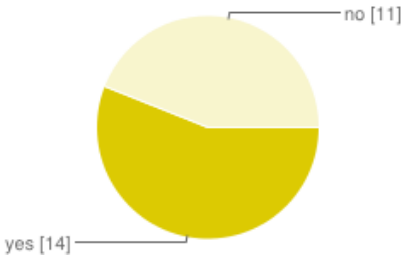


yes	16	64%
no	9	36%

access control to the documents that I shared is set up by

myself - I determine who gets access	8	24%
IT admin -- I give them the list of people who can access	14	41%
my team leader -- I give him the list of potential people who can access	12	35%
everyone gets access to all documents during the course of onboarding	0	0%

Did you have access to all onboarding related documents in the collaboration work space or central repository?



yes	14	56%
no	11	44%

How would someone request access to your documents in the shared work space?

everyone has access to all documents in the work space	1	3%
they send me a request by email to grant them access to my document in the work space	14	44%
the collaboration system has features to request/grant access	17	53%

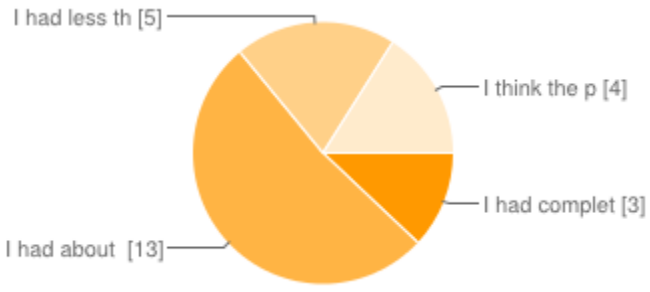
How do you grant access to documents?

everyone has access to all documents in the work space	1	3%
I grant access using the features of the collaboration system to grant/request access	18	55%
I email them the documents that they requested	7	21%
I seek approval of my onboarding team lead	7	21%

Did you access documents in the collaboration work space which were not directly related to your onboarding role?

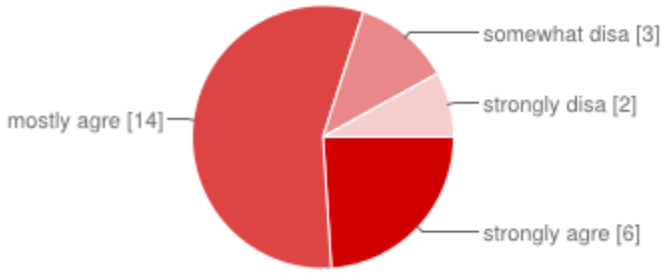
sometimes opened documents accidentally	2	6%
never accessed unrelated documents	6	18%
sometimes opened documents to find out if I needed them	13	39%
I opened other documents to gain broader understanding	12	36%

Did you have clarity about process life cycle of onboarding acquisitions?



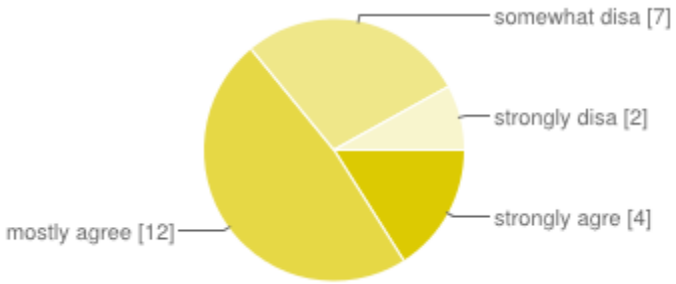
I had complete clarity of process	3	12%
I had about 75% clarity of the process	13	52%
I had less than 50% clarity of process	5	20%
I think the process was not clear at all	4	16%

I know when my role in the onboarding begins and ends



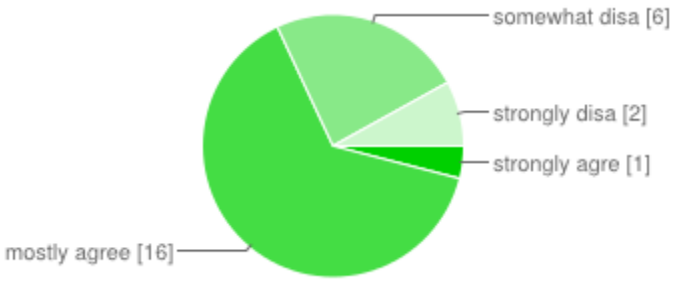
strongly agree	6	24%
mostly agree	14	56%
somewhat disagree	3	12%
strongly disagree	2	8%

For each process step in onboarding acquisition, the roles and responsibilities were clearly defined



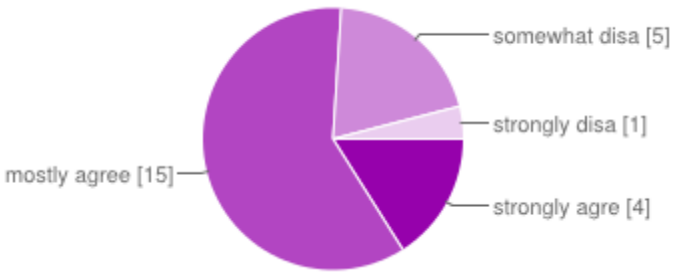
strongly agree	4	16%
mostly agree	12	48%
somewhat disagree	7	28%
strongly disagree	2	8%

The inter-enterprise collaboration process is defined completely and accurately



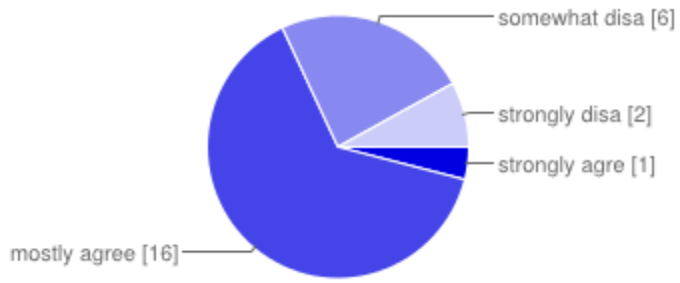
strongly agree	1	4%
mostly agree	16	64%
somewhat disagree	6	24%
strongly disagree	2	8%

The milestones for onboarding process are defined satisfactorily



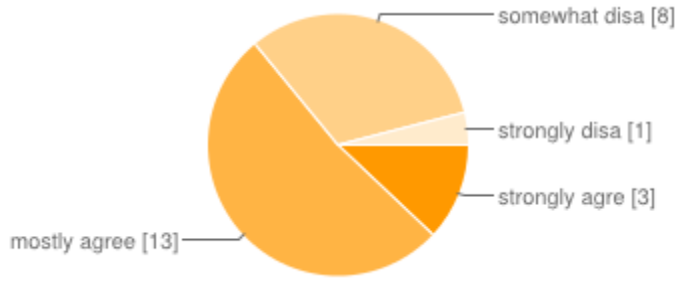
strongly agree	4	16%
mostly agree	15	60%
somewhat disagree	5	20%
strongly disagree	1	4%

The metrics for measurement of onboarding process progress are defined satisfactorily



strongly agree	1	4%
mostly agree	16	64%
somewhat disagree	6	24%
strongly disagree	2	8%

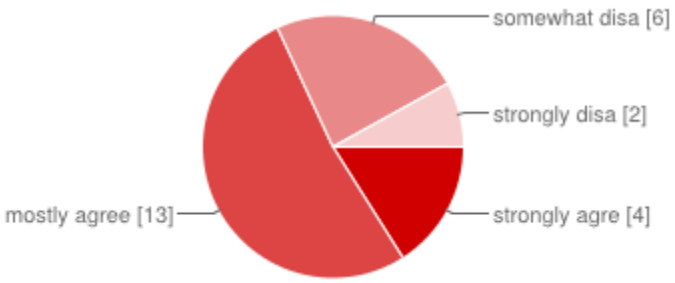
Risk Management strategies are well defined to manage project timelines



strongly agree	3	12%
mostly agree	13	52%
somewhat disagree	8	32%

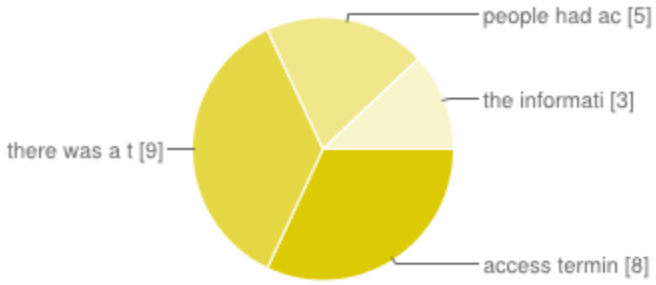
strongly disagree	1	4%

Risk Management strategies are well defined to manage personnel changes during onboarding process



strongly agree	4	16%
mostly agree	13	52%
somewhat disagree	6	24%
strongly disagree	2	8%

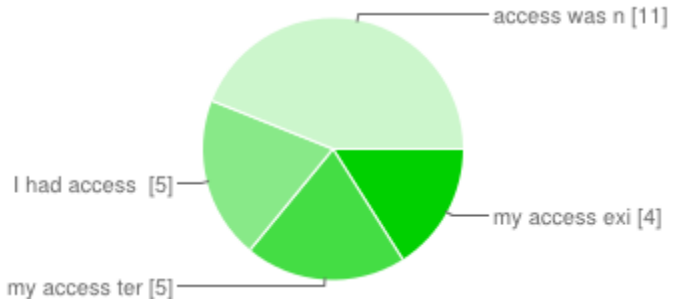
When a person's role ended during collaboration their access to collaboration space was terminated?



access terminated immediately and team got notified	8	32%
there was a time lag in terminating access	9	36%
people had access to collaboration work space even after the onboarding was completed	5	20%

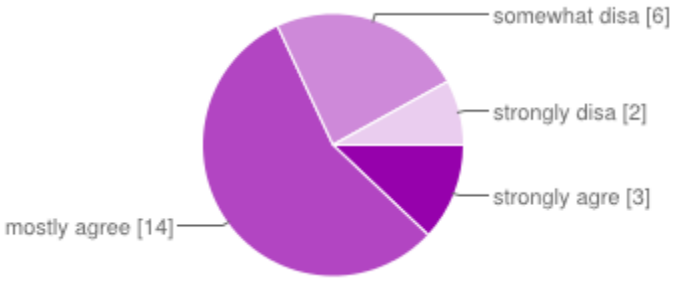
the information about whose role ended was not available	3	12%

I had access to collaboration space even after the onboarding project officially closed



my access existed for at least one month after close of project	4	16%
my access terminated on the day of onboarding project closure	5	20%
I had access for up to a week after onboarding project closure	5	20%
access was never terminated	11	44%

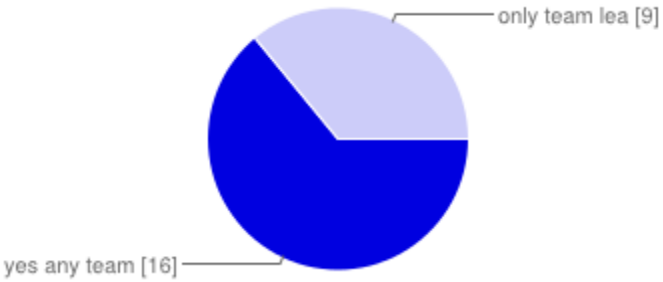
The onboarding project closure is defined clearly



strongly agree	3	12%
mostly agree	14	56%
somewhat disagree	6	24%

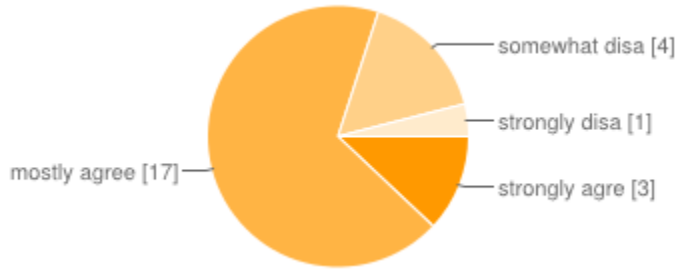
strongly disagree	2	8%

Anyone can put documents in the collaboration work space



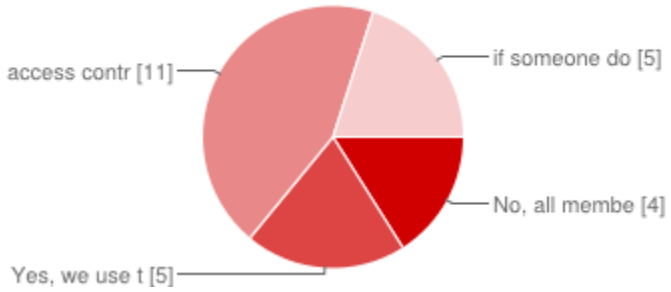
yes any team member can put documents in the workspace	16	64%
only team leader can put documents in the work space	9	36%

The assignment of roles and access control is clearly defined for onboarding process lifecycle



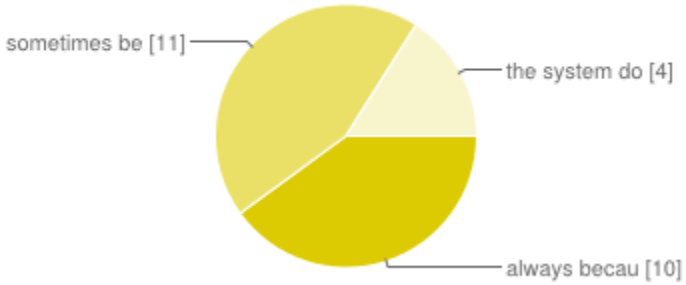
strongly agree	3	12%
mostly agree	17	68%
somewhat disagree	4	16%
strongly disagree	1	4%

Do you use any trust management techniques to grant access to documents in work space?



No, all members have access to documents	4	16%
Yes, we use trust management techniques to determine access dynamically	5	20%
access control is determined by statically defined policies	11	44%
if someone does not have access but I trust them I share the documents	5	20%

I get notifications when new documents are put in the collaboration workspace



always because the system notifies everyone	1 0	40 %
sometimes because the individual who put the document can specify the people who should be notified	1 1	44 %
the system does not have automatic notification mechanisms	4	16

%

In your opinion how effectively collaboration security (in terms of access control) is managed in onboarding acquisitions?

This is an immature area. We use Sharepoint for sharing documents and folders. Mostly for ongoing teams. Once a folder is created and role based access is defined, it remains the same. Onboard and offboarding processes are not yet linked to the collaboration space access protocols. There are some SOX access guidelines, where each quarter, the owner of a folder has to certify the list of users who are no more with the company and remove those who are not with the company. The management is not very mature. Though processes exist and can be managed automatically, a certain amount of manual discretion is used. Not very strong I dont think companies manage access control effectively when managing onboarding acquisitions We use tools for configuration management and collaboration. These tools provide robust security and access controls. So we are able to manage the collaboration security very effectively. not effectively at all. I would use a high, medium, and low framework. I would rate the security as medium. reasonably effective very important In my experience with the XXX acquisition of YYY, collaboration Security was very effectively managed based on XXX's well established processes and procedures. Reasonably well Most of the time it works As part of IT our access to Acquisition documents is controlled at a Team level who has access to all documents pertaining to Acquisition from an IT perspective. The security aspect may not be that much at this time because acquisition decision has already been taken and IT is already involved. The companies I did were less than 200 people on each side. Thus, security actually went very well if the teams wanted to get together. It is like getting married to your counter-part. It gets very personal. Outsiders from other departments that do not have need to know will not be able to get into non-appropriate "clicks". The clicks get very tight. If anything getting to the needed information was the issue, because the clicks on the two sides will have somewhat different boundaries. In my opinion, the collaboration security was poorly managed in onboarding acquisitions. It has mostly been effective. Perhaps, too much caution is used when granting access. These type

environments always run somewhat loose, as is with access control. It's a priority in the thought and docs, but not always implemented in real life. it is not as thought out as it should be at my company In any acquisition process, data is present in two different organizations. Some Employees from either organization need to access data from both sources. Making data available to these audience can be managed effectively. User groups and stakeholders are determined before the collaboration and engagement process is kicked off, allowing for clear visibility of users that will need access to the data and documents There are a set of steps that are expected to be performed when onboarding acquisitions; however, "access control" requirements are not proactively defined. Usually, this requirement is driven by the program manager in business development that is handling the acquisition. It's important to note that the way such access control is defined does vary from one program manager to another. security was managed only at the level of who needs access Satisfactory managed. In my experience, there was no collaboration security in place during the acquisition that I was involved in. Very effectively

What process improvement suggestions you may have for on boarding acquisitions?

Automated integration of new teams onboarded during acquisition and set up the levels of access to the shared folders using a tool. Currently, it is manual. Some training to the personnel involved in the acquisitions on best practices and any software to be used. Well defined roles and responsibilities. Better version controls and access control 1. Clearly define the onboarding process and create an onboarding roadmap 2. Integrate onboarding with overall acquisition process 3. Extend onboarding to the first six months of the acquisition 4. Replace paper and spreadsheet based processes and use an automated system that includes forms management, tasks managements, and socialization in the company culture. 4. Create an onboarding roadmap in order to establish a long-term strategic plan for the onboarding process. Clearly defining the process steps and communicating that to all the stakeholders is very important. a workflow service should be set up to manage the process directly with all members when events happen (based on the event) Provide a clear project management plan that outlines all key stakeholders from the start. Do

not rush the merger since that creates more problems regarding the on-boarding--in short give key stakeholders enough time to plan out the work so everyone is successful. none more regular and structured mtgs with deliverable and action items Communication with the employees in terms of Integration Update. Better dashboards Clearer definitions ahead of the process commencement. Clearer methods to include people quickly that can view and edit docs. IT should be involved from the beginning to make sure IT infrastructure is aligned to the overall Acquisition process. Many times IT gets involved at a later stage with a particular deadline approaching. IT may not have enough time and resources to do its job. Rent an apartment at the other location and rotate the staff often. Each person should go back multiple times as they ramp up their learning curve. Shorter, longer, shorter. The biggest learning is in the middle. Kill off one of the accounting departments. There can only be one set of agreed upon "numbers". Put key members on consulting contracts when they leave - and then actually use the time. *** Above all else protect the computers and networks in engineering, manufacturing and sales. There is no way to rebuild them exactly. A customer support call even 2 years later may require you to turn on the computers to find the answers. Leave special equipment connected!. If you move equipment around you break software licenses and custom in-house scripts. 1. Roles and responsibilities of every team/member involved in onboarding should be identified. 2. The process should be streamlined further to understand the sequence of activities, clear handoffs between teams and the activities that can run in parallel. 3. Personal information of the newly onboarded team/members should be properly secured. 4. While granting access control to information and documents, it should be clearly identified in advance as to who should get what information and in which format. 5. Training the newly onboarded members should be done more effectively so that the new members understand how the training is relevant to them. 6. Maintaining an effective time line is important in onboarding the new team members. There seems to be a certain amount of fear if you're the company who has been acquired. Putting to rest those fears first would be ideal. Keeping and revisiting the documented processes/procedures identified in initial goals, timelines and requirements. define what type of acquisition it is, than have a clear handbook in processes and operating model. There are opportunities to improve in the areas of Collaboration Security. To put an

automated system in place to walk stakeholders through the process, showing clearly what has been done, what has begun, and the KPIs around each step. Develop a consistent process protocol that is simple to initiate and monitor. The application should "encourage" periodic validation to ensure that the access control requirements are still applicable. the team leader should be able to maintain a team roster Better communication between all the different team players. Clarify the team and roles Choose strong decisive team members that see the value in the process Define goals, objectives, metrics for onboarding Develop a timeline Use a dashboard to map progress Have executive sponsors to support the program Be realistic in setting expectations about company culture integration as this takes a long time If budget is available provide culture conditioning for the acquired entity if it is significantly smaller than the new parent company

Anything else you would like to share in terms of onboarding process and collaboration security?

The authentication information (such as Active Directory) should be used as a reference periodically (e.g. daily) against the current user list of a collaboration system to create delta list, and create tasks for adding/removing those users to manage the delta list. Using a tool based approach is very important - especially in a multiple acquisition environment. A strong executive sponsorship is needed to make this overall process successful. tracking is key and we do not have visibility to it NA I was involved in the onboarding process when XXX acquired YYY. XXX has a good track record and experience in m&a and has well defined process for it. None How to minimize duplication of information by proper categorization. How to have a chart of docs / tree that shows the layout of docs and categories. This survey's design vastly under estimates the amount (a) of paper transported back and forth (many hundreds of pounds+ per department), (b) the vast number of hours of the phone, skype, etc. A lot of talking goes on. Many business procedures, practices, and knowledge are not written down. Verbal knowledge can be 1/3rd or more of the stuff you bought. (c) the amount of face-to-face time. It is normal for key people to live at the other places for several weeks. You have to "do it" yourself to really understand. Sale and

marketing still takes face time to build trust and deep understanding. If you don't understand the live human behavior and interaction - you will make mistakes. A webcam is not a substitute for a late night beer. ~ There are situations where sensitivity around the on boarding details should be secured, depending on the how much of the acquisition specifications have been defined and socialized. Tighter security may be required during this Pre-Onboarding / Acquisition phase. There is still much to be gained for improving collaboration security. Ease of use, effectiveness in ensuring that those given access are the only individuals are allowed to view content. no My on-boarding experience occurred in my previous companies, not my current company

May I follow up with you? If so, please give your contact number and email.

Deleted for confidentiality